304-CD-003-002

EOSDIS Core System Project

Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project

This document has not yet been approved by the Government for general use or distribution.

Final

March 1995

Hughes Applied Information Systems
Landover, Maryland

Communications and System Management Segment (CSMS) Requirements Specification for the ECS Project

March 1995

Prepared Under Contract NAS5-60000
CDRL Item 045

SUBMITTED BY

Peter G. O'Neill /s/ 13 Mar 95

Marshall A. Caplan, Project Manager Date
EOSDIS Core System Project

Hughes Applied Information Systems
Landover, Maryland

304-CD-003-002

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code 1. It requires Government review and approval prior to acceptance and use. Changes to this document shall be made by document change notice (DCN) or by complete revision.

CSMS Requirements document is under the control of the CSMS Configuration Control Board (CCB). Changes to this document must be approved by this CCB prior to inclusion in the document.

Once approved, this document shall be under ECS Project Configuration Control.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Applied Information Systems
1616 McCormick Dr.
Landover, MD 20785

This page intentionally left blank.

Abstract

This document specifies the Interim Release 1 (IR-1) and Release A Level-4 requirements for the Communications and System Management Segment.(CSMS) of the ECS Project

Keywords: Level-4, Requirement, Segment Requirement Specification, SRS, CSMS, MSS, CSS, ISS, ECS

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Final
iii through xvi	Final
1-1 and 1-2	Final
2-1 through 2-4	Final
3-1 through 3-6	Final
4-1 through 4-34	Final
5-1 through 5-64	Final
6-1 through 6-44	Final
7-1 through 7-10	Final
A-1 and A-6	Final
B-1 and B-66	Final
C-1 through C-6	Final
D-1 through D-66	Final
AB-1 through AB-6	Final

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
304-CD-003-001	Review Copy	December 1994	
304-CD-003-002	Final	March 1995	95-0114

This page intentionally left blank.

Contents

4. Hardware Requirements

5. MSS Functional Requirements

6. CSS Functional Requirements

7. ISS Functional Requirements

Figures

Tables

1. Introduction

1.1 Scope

This CSMS Requirements Specification defines the CSMS Level 4 requirements for Interim Release 1 (IR-1) and Release A.

These requirements were derived from the Level 3 requirements, as defined in the ECS Functional and Performance Requirements, that map to the functional capability and services defined in the Release Plan Content Description White Paper, FB9403V4. Traceability to these Level 3 requirements will be denoted in Appendix A, Level 4 Traceability Matrix.

This document reflects the Technical Baseline submitted via contract correspondence number ECS 194-00343.

1.2 Document Organization

The document is organized to describe the level 4 Communications and System Management Segment (CSMS) requirements.

Section 1 provides information regarding the identification, scope, status, and organization of this document.

Section 2 provides a listing of the related documents, which were used as source information for this document.

Section 3 provides an overview of the CSMS, focusing on the CSMS high-level operational concept. This provides general background information to put CSMS into context.

Section 4 contains the CSMS hardware requirements.

Section 5 contains the requirements associated with the Management Subsystem (MSS). This includes the Fault Management, Performance Management, Security Management, Accounting Management, Common Management, Configuration Management and Management Agent Services.

Section 6 contains the requirements associated with the Communications Subsystem (CSS). This includes the Common Facilities, Object and Distributed Object Framework Services.

Section 7 contains the requirements associated with the Internetworking Subsystem (ISS).

Appendix A contains the capacity and performance characteristics that were used to derive the network and hardware requirements for Interim Release 1 and Release A.

Appendix B contains the Traceability Matrix for Level 4 requirements to the Level 3 requirements, and the Release.

Appendix C contains the IRD Traceability Matrix to CSMS Level 4 requirements.

Appendix D contains the Traceability Matrix for Level 3 requirements to the Level 4 requirements.

The Abbreviations and Acronyms section contains an alphabetized list of the definitions for abbreviations and acronyms used in this volume.

1.3 CSMS Requirements Specification Configuration Control

CSMS Requirements document is under control of the CSMS Configuration Control Board (CCB).

Changes to this document must be approved by this CCB prior to inclusion in the document.

1.4 Status and Schedule

This submittal of DID 304/DV1 meets the milestone specified in the Contract Data Requirements List (CDRL) of NASA Contract NAS5-60000.

2. Related Documentation

2.1 Parent Document

The parent documents are the documents from which this CSMS Requirements Specification's scope and content are derived.

194-219-SE1-001	Interface Requirements Document Between EOSDIS Core System (ECS) and the NASA Science Internet (NSI)
219-CD-003-001	Interface Requirements Document Between EOSDIS Core System (ECS) and Landsat 7 System, Final
194-219-SE1-004	Interface Requirements Document Between EOSDIS Core System (ECS) and the Version 0 System
194-219-SE1-005	Interface Requirements Document Between EOSDIS Core System (ECS) and Science Computing Facilities
219-CD-006-001	Interface Requirements Document Between EOSDIS Core System (ECS) and Affiliated Data Centers, Final
193-219-SE1-008	Interface Requirements Document Between EOSDIS Core System (ECS) and Program Support Communications Network, Draft, 8/93
194-219-SE1-015	Interface Requirements Document Between EOSDIS Core System (ECS) and International Partners for Data Interoperability, Preliminary (formerly Interface Requirements Document Between EOSDIS Core System (ECS) and The European Space Agency)
194-219-SE1-018	Interface Requirements Document Between EOSDIS Core System (ECS) and Tropical Rainfall Measuring Mission (TRMM) Ground System
194-219-SE1-019	Interface Requirements Document Between EOSDIS Core System (ECS) and Earth Observing System (EOS) AM-1 Flight Operations
194-219-SE1-020	Interface Requirements Document Between EOSDIS Core System (ECS) and NASA Institutional Support Systems
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)
560-EDOS-0211.0001	Goddard Space Flight Center, Interface Requirement Document Between the EOSDIS Data and Operations System (EDOS) and EOS Ground System (EGS) Elements

2.2 Applicable Documents

The following documents are referenced within this CSMS Requirements Specification, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

194-207-SE1-001	System Design Specification for the ECS Project
304-CD-001-002	Flight Operations Segment (FOS) Requirements Specification for the ECS Project, Volume 1: General Requirements
304-CD-004-002	Flight Operations Segment (FOS) Requirements Specification for the ECS Project, Volume 2: Mission Specific
194-604-OP1-001	ECS Operations Concept Document for the ECS Project Working Draft
222-TP-003-005	Release Plan Content Description, White Paper, Working Paper, September 1994. Note: The Release Plan is being updated to reflect changes in the implementation schedule for CORBA-related services.
none	Goddard Space Flight Center, EOS AM-1 Ground Systems Requirements

2.3 Information Documents

The following documents are referenced herein and, amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS CSMS Requirements Specification.

209-CD-003-001	Interface Control Document Between EOSDIS Core System (ECS) and the EOS-AM Project for AM-1 Spacecraft Analysis Software, Preliminary
209-CD-004-001	Data Format Control Document for the ECS Flight Operations Segment AM-1 Project Data Base (PDB) Preliminary
220-CD-001-003	Communications Requirements for the ECS Project, Final
560-EDOS-0230.0001	Goddard Space Flight Center/MO&DSD, Earth Observing System (EOS) Data and Operations System (EDOS) Data Format Requirements Document (DFRD)
530-DFCD-NCCDS/POCC	Goddard Space Flight Center/MO&DSD, Data Format Control Document Between the Goddard Space Flight Center Payload Operations Control Centers and the Network Control Center Data System

502-ICD-JPL/GSFC	Goddard Space Flight Center/MO&DSD, Interface Control Document Between the Jet Propulsion Laboratory and the Goddard Space Flight Center for GSFC Missions Using the Deep Space Network
FIPS PUB 127-1	Federal Information Processing Standards Publication: Database Language SQL
RFC768	J. Postel; User Datagram Protocol, 8/28/80
RFC791	J. Postel; Internet Protocol, 9/1/81 (obsolete/updated by RFC1060)
RFC792	J. Postel; Internet Control Message Protocol, 9/1/91
RFC793	J. Postel; Transmission Control Protocol, 9/1/91
RFC821	J. Postel; Simple Mail Transfer Protocol, 8/1/82
RFC826	D. Plummer; Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, 11/1/82
RFC854	J. Postel, J. Reynolds; Telnet Protocol specifications, 5/1/83
RFC894	C. Hornig; Standard for the Transmission of IP Datagrams Over Ethernet Networks, 4/1/84
RFC895	J. Postel; Standard for the Transmission of IP Datagrams Over Experimental Ethernet Networks, 4/1/84
RFC903	R. Finlayson, et al; Reverse Address Resolution Protocol, 6/1/84
RFC959	J. Postel, J. Reynolds; File Transfer Protocol, 10/1/85
RFC977	B. Kantor, P. Lapsley; Network News Transfer Protocol: A proposed Standards for the Stream-Based Transmission of News, 2/1/86
RFC1058	C. Hedrick; Routing Information Protocol, 6/1/88
RFC1060	J. Postel, J. Reynolds; ASSIGNED NUMBERS, 3/20/90 (obsolete/ updated by RFC1340)
RFC1157	M. Schoffstall, et al; A Simple Network Management Protocol (SNMP), 5/10/90
RFC1188	D. Katz; A Proposed Standard for the Transmission of IP Datagrams over FDDI Networks, 10/30/90 (obsolete/updated by RFC1390)
RFC1209	J. Lawrence, D. Piscitello; The Transmission of IP Datagrams Over the SMDS Service, 3/6/91
RFC1213	K. McCloghrie, M. Rose; Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, 3/26/91

RFC1340	J. Reynolds, J. Postel; ASSIGNED NUMBERS, 7/10/92
RFC1374	J. Renwick, A. Nicholson; IP and ARP on HIPP, 11/2/92
RFC1390	D. Katz; Transmission of IP and ARP over FDDI Networks, 1/5/93
RFC1411	D. Borman; Telnet Authentication: Kerberos Version 4, 1/26/93
RFC1521	N. Borenstein, N. Freed; MIME (Multipurpose Internet Mail Extensions) Part one: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, 9/23/93
RFC1522	K. Moore; MIME (Multiprupose Internet Mail Extensions) Part two: Message Header Extensions for Non-ASCII Text, 9/23/93
RFC1583	J. Moy; OSPF Version 2, 3/23/94
RFC1623	F. Kastenholz; Definitions of Managed Objects for the Ethernet-like Interface Types, 5/24/94

3. Communications and System Management Segment Overview

The Communications and Systems Management Segment (CSMS) accomplishes the interconnection of users and service providers, transfer of information between ECS (and many EOSDIS) components, and enterprise management of all ECS components. It supports and interacts with the Science Data Processing Segment (SDPS) and the Flight Operations Segment (FOS).

The services provided by CSMS at the System Monitoring and Coordination Center, (SMC) located at Goddard Space Flight Center (GSFC), are collectively referred to as Enterprise Monitoring and Coordination (EMC) throughout this document. In the same context, services provided by CSMS at Distributed Active Archive Centers (DAACs) and the EOC (sites) are collectively referred to as Local System Management (LSM).

At its highest design level, CSMS consists of three parts:

- System Management Subsystem (MSS)

  MSS is a collection of applications which manage all ECS resources, including all SDPS, FOS, ISS, and CSS components. MSS directly uses CSS services.

- Communications Subsystem (CSS)

  CSS is a collection of services providing flexible interoperability and information transfer between clients and servers. CSS services correspond loosely to layers 5-7 of the Open Systems Interconnection Reference Model (OSI-RM).

- Internetworking Subsystem (ISS)

  ISS is a layered stack of communications services corresponding to layers 1-4 of the OSI-RM. CSS services reside over, and employ, ISS services.

3.1 Systems Management Subsystem (MSS) Description

The services of the System Management Subsystem (MSS) are depicted in Figure 3-1. The MSS services include management application services, common management services (management framework), and management agent service. The MSS is largely in the application domain, above the OSI-RM application-layer services. Common Management Services and CSS Common Facility and Object Services support the Management Application Services Additionally, MSS is functionally dependent upon the services of the Internetworking Subsystems. Section 5 describes the functional requirements of the System Management Subsystem.

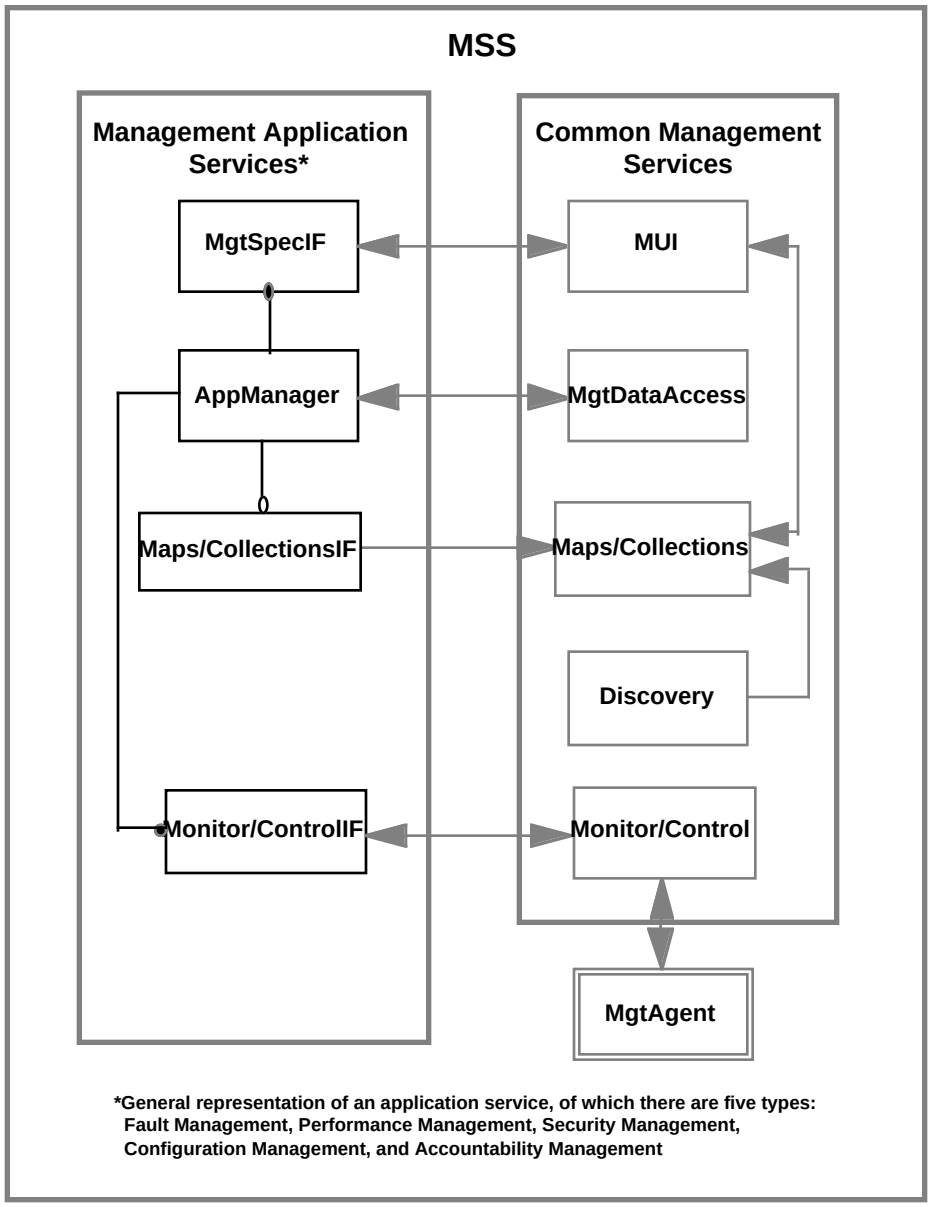

Figure 3-1. MSS Subsystem Diagram

3.2 Communications Subsystem (CSS) Description

Service superclasses and classes of the Communications Subsystem (CSS) are depicted in Figure 3-2. The CSS superclasses are distributed object framework services, object services, and common facility services. From an open systems interconnection-reference model (OSI-RM, or ISO 7498:1994, Open Systems Interconnection) perspective, the Communications Subsystem is comprised of layers 5-7, the session, presentation, and applications layers. Support in this subsystem area is provided for peer-to-peer, client/server, messaging, management, and event-handling communications facilities. These services typically appear on communicating end systems across an internetwork and are not layered, but hierarchical in nature. Additionally, services within OSI-RM layers 5-7 to support communicating entities are provided, included directory, security, time, and other ancillary services. The services of the Communications Subsystem are functionally dependent on the services of the Internetworking Subsystem. Many of the common facilities may be jointly developed by CSMS with the other segments. The services of the common facility, object and distributed object framework superclasses are the fundamental set of interfaces for all CSMS management and FOS and SDPS user access (i.e., pull) domain services. The distributed object framework services are the fundamental set of dependencies of the common facility and object services. Section 6 describes the functional requirements of the Communications Subsystem.

3.3 Internetworking Subsystem (ISS) Description

The Internetworking Subsystem provides for the transfer of data transparently between end systems within local and wide area networks. The primary aspects of ISS development include:

- selection of internetworking protocols and standards to be used to satisfy ECS requirements;
- selection of vendor implementation of chosen protocols and standards; and
- design of internetworking topology.

ECS is responsible for designing and developing both the EOSDIS Science Network (ESN) Local area networks (LANs) and the ESN Wide Area Network (WAN). The ESN LANs are responsible for transfer of data within the DAACs, SMC and EOC, and for providing interfaces between these components and to external networks. The ESN WAN's primary function is to transfer data between DAACs, including both product data and inter-DAAC queries and metadata responses. Other networks, including Ecom, Nascom, and NSI, will provide wide-are services to ECS. In addition, "campus" networks, which form the existing networking infrastructure at the ECS locations, will provide connectivity to EOSDIS components such as Science Computing Facilities (SCFs) and Instrument Support Terminals (ISTs).

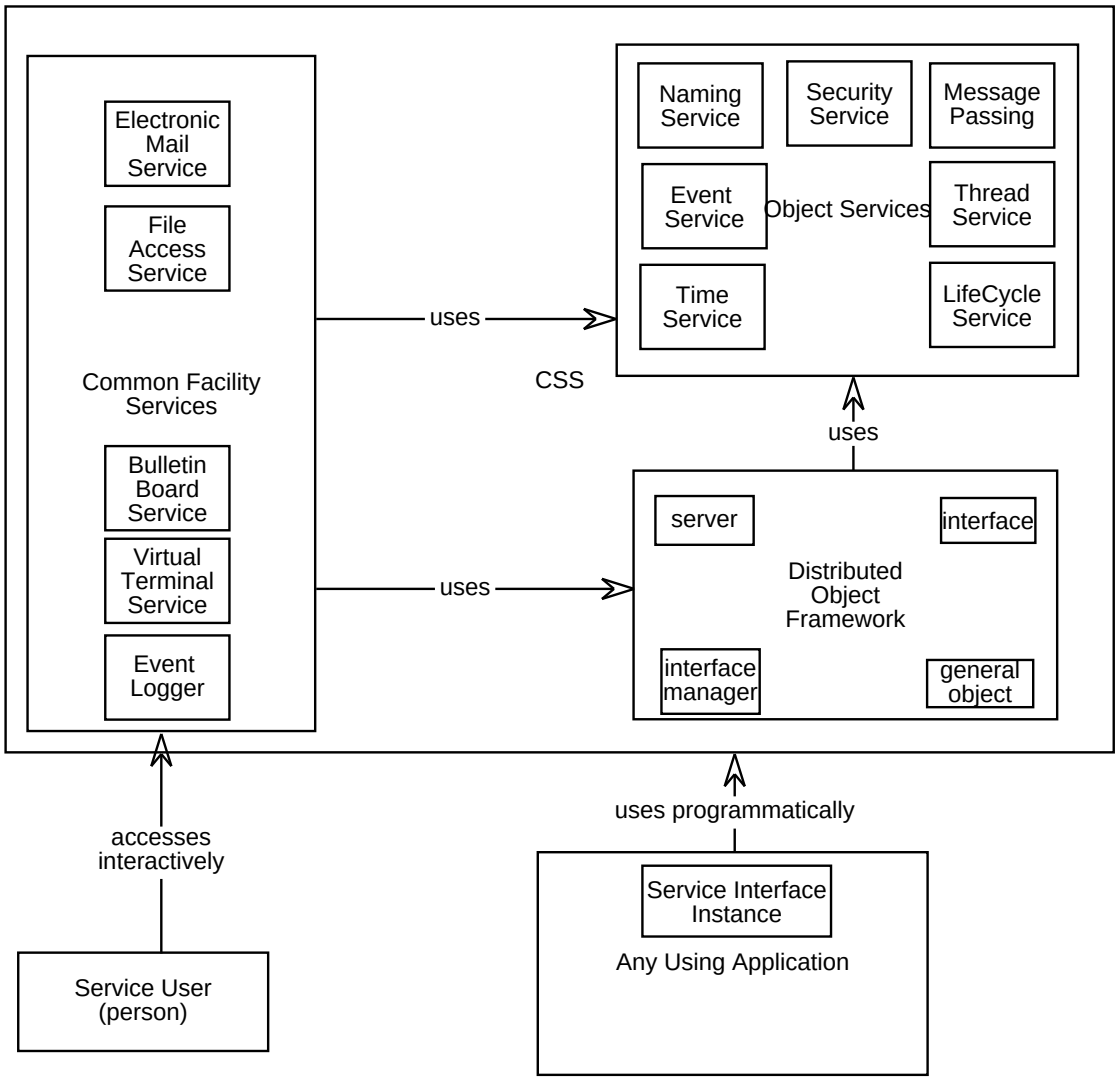

Figure 3-2. CSS Subsystem Diagram

3.4 CSMS Configuration Items (CIs)

The service class mappings to the CSMS Configuration Items (CIs) for IR-1 and Release A are shown in Table 3.4-1.

The Systems Management Subsystem (MSS) common management services and management application services map to the Management CI (MCI), the Management Logistics CI (MLCI), the Management Agent CI (MACI), and the MSS Management Hardware CI (MHCI). The MHCI includes site specific configurations of workstations and servers for management of DAACs, EOC/ICC, for WAN management, and for system-wide coordination and monitoring purposes.

The Communications Subsystem (CSS), comprised of three service superclasses, is mapped to the Distributed Computing CI (DCCI), and the Distributed Communications Hardware CI (DCHCI). All or parts of the DCCI are installed at every ECS machine to enable distributed communications. Machines are configured as clients and/or servers to meet specific implementation requirements. The DCHCI includes communication servers for security, directory, mail, and bulletin board services (software servers may share a physical server) as required to support specific site implementations.

The Internetworking Subsystem (ISS) includes three superclasses which are mapped to the Network CI (NWCI), and the Internetworking Hardware CI (INHCI). Part or all of the NWCI is installed on every ECS machine (end system), and on communication routers (intermediate systems) based on specific site implementation requirements. The INHCI includes routers, plant cabling (e.g., copper cables and optical fiber), and modem access devices required to support specific site implementations.

The Subsystem Superclasses are composed of aggregations of individual service classes. Table 3.4-1 lists these service classes and indicates the mapping of these service classes to the Software CIs. The Service Superclass, CSMS Subsystem and hardware CI (if any) associated with a service class are also provided.

Table 3.4-1. Service Class Mappings to CSMS CIs

Sub System	Service Superclass	Service Class	CI Map
MSS	Common Mgmt. Services	MUI	MCI, MHCI
MSS	Common Mgmt. Services	Agents	MACI
MSS	Common Mgmt. Services	Maps/Collections	MCI, MHCI
MSS	Common Mgmt. Services	Monitor/Control	MCI, MHCI
MSS	Common Mgmt. Services	Discovery	MCI, MHCI
MSS	Common Mgmt. Services	Management Data Access	MCI, MHCI
MSS	Mgmt. Application Services	Fault Resolution Management	MCI, MHCI
MSS	Mgmt. Application Services	Performance Management	MCI, MHCI
MSS	Mgmt. Application Services	Security Management	MCI, MHCI
MSS	Mgmt. Application Services	Configuration Management	MLCI, MHCI
MSS	Mgmt. Application Services	Accounting Management	MCI, MHCI
CSS	Common Facilities	File Access	DCCI, DCHCI
CSS	Common Facilities	Electronic Mail	DCCI, DCHCI
CSS	Common Facilities	Virtual Terminal	DCCI
CSS	Common Facilities	Bulletin Board	DCCI, DCHCI
CSS	Common Facilities	Help Facilities	DCCI
CSS	Object Services	Event	DCCI
CSS	Object Services	Naming	DCCI, DCHCI
CSS	Object Services	LifeCycle	DCCI
CSS	Object Services	Security	DCCI, DCHCI
CSS	Object Services	Persistence	DCCI
CSS	Object Services	Trading	DCCI
CSS	Object Services	Threads	DCCI
CSS	Object Services	Time	DCCI
CSS	Object Services	Archive	DCCI
CSS	Object Services	Backup/Restore	DCCI
CSS	Object Services	Startup/Shutdown	DCCI
CSS	Object Services	Installation/Activation	DCCI
CSS	Distributed Object Framework	Object Frame Work	DCCI
ISS	Transport	Transport	NWCI
ISS	Network	Network	NWCI, INHCI
ISS	Data Link/Physical	Data Link/Physical	NWCI, INHCI

4. Hardware Requirements

This section delineates the segment level requirements for the CSMS hardware. The segment level requirements provide enough detail to implement the CSMS hardware configuration.

This section is organized as follows:

4.1 MSS Management Hardware Configuration Item

4.1.1 Overview of MSS-MHCI

The MSS Management Hardware CI (MSS-MHCI) is the hardware to host all MSS software described in Section 5. The MSS-MHCI logically includes an enterprise system monitoring server, local system management servers, management workstations, and printers.

4.1.2 MSS-MHCI Functional Requirements

4.1.2.1 Monitoring Server

The Enterprise Monitoring Server will provide processors and peripheral equipment necessary for monitoring system and network performance and usage for the entire ECS as required by the CSMS system design. The Enterprise Monitoring Server will be cross-strapped with the Enterprise Communications Server for redundancy, and will coordinate with numerous Local System Management Servers to prevent a single point of failure. The Enterprise Monitoring Server does not interfere with operational processes during normal operations, and preserves DAAC autonomy in operations.

C-HRD-11000 The Enterprise Monitoring Server shall be physically and functionally identical to the Enterprise Communications Server in supporting the CSMS requirements.

C-HRD-11005 The Enterprise Monitoring Server shall share data with the Local System Management Server in supporting the CSMS requirements.

C-HRD-11010 The Enterprise Monitoring Server shall preserve DAAC autonomy of operations.

C-HRD-11015 The Enterprise Monitoring Server shall host the MSS software configuration items to create, with the Enterprise Communications Server and Management Workstations, an enterprise monitoring and coordination center for the ECS.

4.1.2.1.1 Processor

C-HRD-11100 The Enterprise Monitoring Server processor shall include a dedicated terminal to be used as a local systems operations console.

C-HRD-11105 The Enterprise Monitoring Server processor shall be capable of expansion with additional quantities and types of peripherals.

C-HRD-11110 The Enterprise Monitoring Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.

C-HRD-11115 The Enterprise Monitoring Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-11120 The Enterprise Monitoring Server processor terminal shall be compatible with the Management Workstation display device.

4.1.2.1.2 Data Storage/Archive

Data storage/archive for the Enterprise Monitoring Server is a combination of RAID for operational data, and ECS Data Server archival of long-term mission data. The combined data storage/archive will have the capacity to meet CSMS requirements.

C-HRD-11300 The Enterprise Monitoring Server data storage shall be compatible with POSIX compliant operating systems from several vendors.

C-HRD-11310 The Enterprise Monitoring Server data storage shall be compatible with the Local System Management Server short-term data storage.

C-HRD-11315 The Enterprise Monitoring Server data storage shall support RAID level-5: striping with interleaved parity.

C-HRD-11320 The Enterprise Monitoring Server data storage shall have the following hot swappable components:

a. Disks

b. Power Supplies

c. Fans

d. Disk-array controllers

C-HRD-11325 The Enterprise Monitoring Server data storage shall be cross-strapped with the Enterprise Communications Server data storage in supporting the CSMS requirements.

C-HRD-11335 The Enterprise Monitoring Server data storage shall be capable of archiving data to the ECS data server archive for data archive.

C-HRD-11345 The Enterprise Monitoring Server data archive shall adhere to ECS data server archival requirements for data storage and retrieval.

4.1.2.1.3 Peripherals

4.1.2.1.3.1 Local Disk Drives

The Enterprise Monitoring Server disk drives will have the capacity to meet Enterprise Monitoring Server operational requirements for report generation and system analysis.

C-HRD-11505 The Enterprise Monitoring Server peripheral disk drives shall be capable of retrieving data stored from both the enterprise monitoring server data storage and data archive.

4.1.2.1.3.2 Local Tape Drive

Enterprise Monitoring Server tape drives will support Enterprise Monitoring Server data storage and retrieval requirements.

C-HRD-11530 The Enterprise Monitoring Server peripherals shall support at least one tape drive.

C-HRD-11535 The Enterprise Monitoring Server peripheral tape drive shall have the following characteristics:

a. 4mm Digital Audio Tape format

b. Accept industry standard magnetic 4mm DAT (i.e. DDS-90)

c. Data transfer rate of 200KB/sec

C-HRD-11540 The Enterprise Monitoring Server tape drives shall be upgradeable/replaceable within the same product family.

4.1.2.1.3.3 Local CD-ROM Drive

Enterprise Monitoring Server CD-ROM drives will support Enterprise Monitoring Server system software installation and retrieval requirements.

C-HRD-11565 The Enterprise Monitoring Server peripherals shall support at least one CD-ROM drive.

C-HRD-11570 The Enterprise Monitoring Server peripheral CD-ROM drive shall have the following characteristic:

a. Accept 600MB Compact Disk

C-HRD-11575 The Enterprise Monitoring Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.

4.1.2.1.4 Hardware Cabinet

It is desirable, but not mandatory, for the Enterprise Monitoring Server to be housed within one or more standard 19-inch width electronic equipment cabinets. The use of cabinets is an implementation issue dependent on available space at the SMC, DAACs, and EOC; and cost considerations. It is acknowledged that certain vendor platform costs may increase substantially if 19-inch mounting cabinets are made a requirement for procurement. The following are a list of desirable features for the MSS-MHCI Enterprise Monitoring Server hardware. In lieu of equipment cabinets, installation of hardware should adhere to site-specific installation procedures and considerations for power, grounding, and ventilation.

1. The Enterprise Monitoring Server hardware cabinet should house the Enterprise Monitoring Server processor, data storage, and peripherals.
2. The Enterprise Monitoring Server hardware cabinet should provide a RETMA standard 19 inches of equipment mounting width.
3. The Enterprise Monitoring Server hardware cabinet should be a minimum of 54" and a maximum of 72" tall, with standard 19" rack mounts.
4. The Enterprise Monitoring Server hardware cabinet should provide a minimum of 24 inches of equipment mounting depth.
5. The Enterprise Monitoring Server hardware cabinet should accommodate EIA Universal Standard RS-310 hole spacing or provide for a continuously adjustable equipment and panel mounting system.
6. The Enterprise Monitoring Server hardware cabinet should provide removable side panels and rear door.
7. The Enterprise Monitoring Server hardware cabinet should provide earth continuity for all components within.
8. The Enterprise Monitoring Server hardware cabinet should provide sufficient equipment ventilation.
9. The Enterprise Monitoring Server hardware cabinet should supply a minimum of one power controller.

4.1.2.2 Local Management Server

The Local Management Server will provide processors and peripheral equipment necessary for managing system performance and usage for individual DAAC domains as required by the CSMS system design. The Local Management Server will be cross-strapped with the Local Communications Server for redundancy, and will coordinate with the Enterprise Monitoring Server to prevent a single point of failure. The Local Management Server does not interfere with operational processes during normal operations, and preserves other DAAC autonomy in operations.

C-HRD-12000 The Local Management Server shall be physically and functionally identical to the Local Communications Server in supporting the CSMS requirements.

C-HRD-12005 The Local Management Server shall share data with the Enterprise Monitoring Server in supporting the CSMS requirements.

C-HRD-12010 The Local Management Server shall manage only the local DAAC and preserve other DAAC autonomy of operations.

C-HRD-12015 The Local Management Server shall host the MSS software configuration items to create, with the Local Communications Server and Management Workstations, a local system management center for each ECS DAAC.

4.1.2.2.1 Processor

C-HRD-12100 The Local Management Server processor shall include a dedicated terminal to be used as a local systems operations console.

C-HRD-12105 The Local Management Server processor shall be capable of expansion with additional quantities and types of peripherals.

C-HRD-12110 The Local Management Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.

C-HRD-12115 The Local Management Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-12120 The Local Management Server processor terminal shall be compatible with the Management Workstation display device.

4.1.2.2.2 Data Storage/Archive

Data storage/archive for the Local Management Server is a combination of RAID for operational data, and ECS Data Server archival of long term mission data. The data storage/archive will have the capacity to meet CSMS requirements.

C-HRD-12300 The Local Management Server data storage shall be compatible with POSIX compliant operating systems from several vendors.

C-HRD-12310 The Local Management Server data storage shall be compatible with the Enterprise Monitoring Server intermediate-term data storage.

C-HRD-12315 The Local Management Server data storage shall support RAID level-5: striping with interleaved parity.

C-HRD-12320 The Local Management Server data storage shall have the following hot swappable components:

a. Disks

b. Power Supplies

c. Fans

d. Disk-array controllers

C-HRD-12325 The Local Management Server data storage shall be cross-strapped with the Local Communications Server short-term data storage in supporting the CSMS requirements.

C-HRD-12335 The Local Management Server data storage shall be capable of archiving data to the ECS Data Server archive for data archive.

C-HRD-12345 The Local Management Server data archive shall adhere to ECS Data Server archival requirements for data storage and retrieval.

4.1.2.2.3 Peripherals

4.1.2.2.3.1 Local Disk Drives

The Local Management Server disk drives will have the capacity to meet Local Management Server operational requirements for report generation and system analysis.

C-HRD-12505 The Local Management Server peripheral disk drives shall be capable of retrieving data stored from both the Local Management server data storage data archive.

4.1.2.2.3.2 Local Tape Drive

Local Management Server tape drives will support Local Management Server data storage and retrieval requirements.

C-HRD-12530 The Local Management Server peripherals shall support at least one tape drive.

C-HRD-12535 The Local Management Server peripheral tape drive shall have the following characteristics:

a. 4mm Digital Audio Tape format

b. Accept industry standard magnetic 4mm DAT (i.e. DDS-90)

c. Data transfer rate of 200KB/sec

C-HRD-12540 The Local Management Server tape drives shall be upgradeable/ replaceable within the same product family.

4.1.2.2.3.3 Local CD-ROM Drive

Local Management Server CD-ROM drives will support Local Management Server system software installation and retrieval requirements.

C-HRD-12565 The Local Management Server peripherals shall support at least one CD-ROM drive.

C-HRD-12570 The Local Management Server peripheral CD-ROM drive shall have the following characteristic:

a. Accept 600MB Compact Disk

C-HRD-12575 The Local Management Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.

4.1.2.2.4 Hardware Cabinet

It is desirable, but not mandatory, for the Local Management Server to be housed within one or more standard 19-inch width electronic equipment cabinets. The use of cabinets is an implementation issue dependent on available space at the SMC, DAACs, and EOC; and cost considerations. It is acknowledged that certain vendor platform costs may increase substantially if 19-inch mounting cabinets are made a requirement for procurement. The following are a list of desirable features for the MSS-MHCI Local Management Server hardware. In lieu of equipment cabinets, installation of hardware should adhere to site-specific installation procedures and considerations for power, grounding, and ventilation.

1. The Local Management Server hardware cabinet should house the Local Management Server processor, data storage, and peripherals.
2. The Local Management Server hardware cabinet should provide a RETMA standard 19 inches of equipment mounting width.
3. The Local Management Server hardware cabinet should be a minimum of 54" and a maximum of 72" tall, with standard 19" rack mounts.
4. The Local Management Server hardware cabinet should provide a minimum of 24 inches of equipment mounting depth.
5. The Local Management Server hardware cabinet should accommodate EIA Universal Standard RS-310 hole spacing or provide for a continuously adjustable equipment and panel mounting system.
6. The Local Management Server hardware cabinet should provide removable side panels and rear door.

7. The Local Management Server hardware cabinet should provide earth continuity for all components within.
8. The Local Management Server hardware cabinet should provide sufficient equipment ventilation.
9. The Local Management Server hardware cabinet should supply a minimum of one power controller.

4.1.2.3 Management Workstations

The Management Workstations will provide processors and peripheral equipment necessary for system administrator and engineer/analyst access to system performance and usage for individual DAAC domains and the overall ECS enterprise as required by the CSMS system design. The management workstations will not interfere with operational processes. Pools of management workstations at the SMC and all LSMs off-load the servers and allow off-line analysis of management historical data.

C-HRD-13000 All Management Workstations and processors shall be capable of operating simultaneously and independently of other workstations and management/communications servers.

4.1.2.3.1 Processor

Management Workstations will be provided to support enterprise monitoring and local system management operations by system administrators, schedulers, engineers, and analysts.

C-HRD-13100 At a minimum, each processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-13105 Each Management Workstation shall provide one QWERTY keyboard which shall:

a. Be detachable and cabled for movement on a desk-top style workstation area

b. Provide a minimum of 12 programmable function keys

C-HRD-13110 Each Management Workstation shall provide one color text and graphics display device which shall:

a. Display the complete ASCII character set

b. Provide a minimum of 1024 pixel x 864 lines resolution display

c. Display a minimum of 16 colors

d. Display pages 24 lines by 80 characters wide

e. Display a minimum of four screen display pages

f. Display pages readable from any location along the width of the workstation and up to a distance of 6 feet from the screen

g. Provide a minimum of 19 inches diagonal non-glare screen

h. Provide RGB video output for hard copy

i. Feature an integral swivel/tilt base

j. Provide brightness, contrast and power controls within easy reach.

k. Be physically relocatable within the operations center

C-HRD-13115 The Management Workstation shall provide one cursor pointing device (mouse)

C-HRD-13120 The Management Workstation shall be upgradeable/replaceable within the same product family.

4.1.2.3.2 Data Storage

Data for the Management Workstation is pulled from either the Local Management Server and/or Enterprise Monitoring Server data storage. Once pulled from these Servers, the data may be locally stored and manipulated at the Management Workstation.

C-HRD-13300 The Management Workstation data storage shall be capable of retrieving data from the data storage function of both the Enterprise Monitoring Server and the Local Management Server.

4.1.2.3.3 Peripherals

The Management Workstation disk drives will have the capacity to meet Management Workstation requirements for retrieving and analyzing management historical data.

C-HRD-13505 All Management Workstation disk drives serving a specific function (e.g. local management, enterprise monitoring) shall be identical and will have equal capacity.

4.1.2.3.4 Management Workstation Furniture

The following are desirable, but not mandatory features for management workstation furniture. It is acknowledged that the workstation furniture is GFE to the ECS contract. The EMC and LSM management workstations are envisioned as fully integrated Management Workstations, based on human engineering requirements in accordance with MIL-STD-1472C "Human Engineering Design Criteria for Military Systems, Equipment, and Facilities".

1. Each Management Workstation should be equipped with:
   a. One Management Workstation Processor
   b. One printer (shared among Management Workstations)

c. At least eight square feet of clear workspace at desk top height

2. The Management Workstation furniture should include storage compartments to provide mounting space for workstation equipment and storage space for manuals and reference data.
3. The Management Workstation furniture should not significantly obstruct an operator's view of other operational activities.
4. All delivered Management Workstation furniture should be of identical style and material construction.
5. The Management Workstation furniture should be constructed of materials that inhibit the build-up of static electricity and resist corrosion.
6. The Management Workstation furniture should not be damaged by common liquid spills, and shall be designed to protect internally mounted electronics against spills.
7. The Management Workstation furniture exterior texture and finish should minimize glare, reflections, and present an aesthetic, professional appearance for public and official visibility.
8. The Management Workstation furniture should contain provisions for 115 VAC power outlets, and ground stud for connection to the system ground.

4.1.2.4 Printers

The EOC will provide high-speed printers capable of printing enterprise monitoring and local management events, snaps, dumps and listings. Shared system printers will be available for the operations personnel using the Management Workstations. These will be directly attached to the network, providing a pool of printers for all Management Workstations.

C-HRD-13900 Each Printer shall be physically and functionally identical in supporting the CSMS printing requirements.

4.1.3 MSS-MHCI Performance Requirements

C-HRD-16000 The Enterprise Monitoring Server shall be capable of 100 percent growth in Appendix A processing speed without modifications or upgrades to software.

C-HRD-16005 The Enterprise Monitoring Server shall be capable of 100 percent growth in Appendix A storage capacity without modifications or upgrades to software.

C-HRD-16010 The Local Management Server shall be capable of 100 percent growth in Appendix A processing speed without modifications or upgrades to software.

C-HRD-16015 The Local Management Server shall be capable of 100 percent growth in Appendix A storage capacity without modifications or upgrades to software.

C-HRD-16020 The Enterprise Monitoring Server shall be capable of meeting the capacity and performance characteristics of Appendix A.

C-HRD-16025 The Local Management Server shall be capable of meeting the capacity and performance characteristics of Appendix A for all DAAC configurations

C-HRD-16030 The Management Workstation shall be capable of meeting the capacity and performance characteristics of Appendix A.

4.1.4 MSS-MHCI Security Requirements

C-HRD-17000 The MSS-MHCI hardware selection criteria shall meet overall ECS security policies and system requirements.

4.1.5 MSS-MHCI RMA Requirements

C-HRD-18000 The MSS-MHCI Enterprise Monitoring Server shall maintain one backup of all software and key data items in a separate physical location.

C-HRD-18005 The MSS-MHCI Local Management Server shall maintain one backup of all software and key data items in a separate physical location.

C-HRD-18010 The MSS-MHCI functional string between the Enterprise Monitoring Server and the Local Management Server shall provide a function Ao (operational availability) of 0.998 and an MDT of 20 minutes.

C-HRD-18015 The MSS-MHCI functional string between the Local Management Server and ECS managed objects shall provide a function Ao of 0.998 and an MDT of 20 minutes.

4.1.6 MSS-MHCI Evolvability Requirements

There are no L3 evolvability requirements directly allocated to MSS hardware.

4.2 CSS Distributed Communications Hardware Configuration Item

4.2.1 Overview of CSS-DCHCI

The CSS Distributed Communications Hardware CI (CSS-DCHCI) is the hardware to host all CSS software described in Section 6. The CSS-DCHCI logically includes an enterprise communications server, a local communications server, a bulletin board server, and for Release B, a terminal access server.

4.2.2 CSS-DCHCI Functional Requirements

4.2.2.1 Enterprise Communications Server

The Enterprise Communications Server will provide processors and peripheral equipment necessary for enabling distributed communications for the entire ECS as required by the CSMS system design. The Enterprise Communications Server will be cross-strapped with the Enterprise Monitoring Server for redundancy, and will coordinate with numerous Local Communications Servers to prevent a single point of failure. The Enterprise Communications Server preserves DAAC autonomy in the assignment of user authentication and authorization privileges.

C-HRD-21000 The Enterprise Communications Server shall be physically and functionally identical to the Enterprise Monitoring Server in supporting the CSMS requirements.

C-HRD-21005 The Enterprise Communications Server shall share data with the Local Communications Server in supporting the CSMS requirements.

C-HRD-21010 The Enterprise Communications Server shall preserve DAAC autonomy of operations.

C-HRD-21015 The Enterprise Communications Server shall host the CSS software configuration items to create, with the Enterprise Monitoring Server and Management Workstations, an enterprise monitoring and coordination center for the ECS.

4.2.2.1.1 Processor

C-HRD-21100 The Enterprise Communications Server processor shall include a dedicated terminal to be used as a local systems operations console.

C-HRD-21105 The Enterprise Communications Server processor shall be capable of expansion with additional quantities and types of peripherals.

C-HRD-21110 The Enterprise Communications Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.

C-HRD-21115 The Enterprise Communications Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-21120 The Enterprise Communications Server processor terminal shall be compatible with the Management Workstation display device.

4.2.2.1.2 Data Storage/Archive

Data storage/archive for the Enterprise Communications Server is a combination of RAID for operational data, and ECS Data Server archival of long-term mission data. The combined data storage/archive will have the capacity to meet CSMS requirements.

C-HRD-21300 The Enterprise Communications Server data storage shall be compatible with POSIX compliant operating systems from several vendors.

C-HRD-21310 The Enterprise Communications Server data storage shall be compatible with the Communications Server short-term data storage.

C-HRD-21315 The Enterprise Communications Server data storage shall support RAID level-5: striping with interleaved parity.

C-HRD-21320 The Enterprise Communications Server data storage shall have the following hot swappable components:

a. Disks

b. Power Supplies

c. Fans

d. Disk-array controllers

C-HRD-21325 The Enterprise Communications Server data storage shall be cross-strapped with the Enterprise Monitoring Server data storage in supporting the CSMS requirements.

C-HRD-21335 The Enterprise Communications Server data storage shall be capable of archiving data to the ECS Data Server archive for data archive.

C-HRD-21345 The Enterprise Communications Server data archive shall adhere to ECS data server archival requirements for data storage and retrieval.

4.2.2.1.3 Peripherals

4.2.2.1.3.1 Local Disk Drives

The Enterprise Communications Server disk drives will have the capacity to meet Enterprise Communications Server operational requirements for report generation and system analysis.

C-HRD-21505 The Enterprise Communications Server peripheral disk drives shall be capable of retrieving data stored from both the Enterprise Communications server data storage and data archive.

4.2.2.1.3.2 Local Tape Drive

Enterprise Communications Server tape drives will support Enterprise Communications Server data storage and retrieval requirements.

C-HRD-21530 The Enterprise Communications Server peripherals shall support at least one tape drive.

C-HRD-21535 The Enterprise Communications Server peripheral tape drive shall have the following characteristics:

a. 4mm Digital Audio Tape format

b. Accept industry standard magnetic 4mm DAT (i.e. DDS-90)

c. Data transfer rate of 200KB/sec

C-HRD-21540 The Enterprise Communications Server tape drives shall be upgradeable/replaceable within the same product family.

4.2.2.1.3.3 Local CD-ROM Drive

Enterprise Communications Server CD-ROM drives will support Enterprise Communications Server system software installation and retrieval requirements.

C-HRD-21565 The Enterprise Communications Server peripherals shall support at least one CD-ROM drive.

C-HRD-21570 The Enterprise Communications Server peripheral CD-ROM drive shall have the following characteristic:

a. Accept 600MB Compact Disk

C-HRD-21575 The Enterprise Communications Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.

4.2.2.1.4 Hardware Cabinet

It is desirable, but not mandatory, for the Enterprise Communications Server to be housed within one or more standard 19-inch width electronic equipment cabinets. The use of cabinets is an implementation issue dependent on available space at the SMC, DAACs, and EOC; and cost considerations. It is acknowledged that certain vendor platform costs may increase substantially if 19-inch mounting cabinets are made a requirement for procurement. The following are a list of desirable features for the CSS-DCHCI Enterprise Communications Server hardware. In lieu of equipment cabinets, installation of hardware should adhere to site-specific installation procedures and considerations for power, grounding, and ventilation.

1. The Enterprise Communications Server hardware cabinet should house the Enterprise Communications Server processor, data storage, and peripherals.
2. The Enterprise Communications Server hardware cabinet should provide a RETMA standard 19 inches of equipment mounting width.
3. The Enterprise Communications Server hardware cabinet should be a minimum of 54" and a maximum of 72" tall, with standard 19" rack mounts.
4. The Enterprise Communications Server hardware cabinet should provide a minimum of 24 inches of equipment mounting depth.
5. The Enterprise Communications Server hardware cabinet should accommodate EIA Universal Standard RS-310 hole spacing or provide for a continuously adjustable equipment and panel mounting system.
6. The Enterprise Communications Server hardware cabinet should provide removable side panels and rear door.
7. The Enterprise Communications Server hardware cabinet should provide earth continuity for all components within.
8. The Enterprise Communications Server hardware cabinet should provide sufficient equipment ventilation.
9. The Enterprise Communications Server hardware cabinet should supply a minimum of one power controller.

4.2.2.2 Local Communications Server

The Local Communications Server will provide processors and peripheral equipment necessary for enabling distributed communications within a local DAAC as required by the CSMS system design. The Local Communications Server will be cross-strapped with the Local Management Server for redundancy, and will coordinate with the Enterprise Communications Server to prevent a single point of failure. The Local Communications Server preserves DAAC autonomy in the assignment of user authentication and authorization privileges.

C-HRD-22000 The Local Communications Server shall be physically and functionally identical to the Local Management Server in supporting the CSMS requirements.

C-HRD-22005 The Local Communications Server shall share data with the Enterprise Communications Server in supporting the CSMS requirements.

C-HRD-22010 The Local Communications Server shall be configurable according to local DAAC user authentication/authorization policy and preserve other DAAC autonomy of operations.

C-HRD-22015 The Local Communications Server shall host the CSS software configuration items to create, with the Local Management Server and Management Workstations, a local system management center for each ECS DAAC.

4.2.2.2.1 Processor

C-HRD-22100 The Local Communications Server processor shall include a dedicated terminal to be used as a local systems operations console.

C-HRD-22105 The Local Communications Server processor shall be capable of expansion with additional quantities and types of peripherals.

C-HRD-22110 The Local Communications Server processor shall be upgradeable/replaceable within the same product family without major software modification or replacement of any peripheral or attached component.

C-HRD-22115 The Local Communications Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-22120 The Local Communications Server processor terminal shall be compatible with the Management Workstation display device.

4.2.2.2.2 Data Storage/Archive

Data storage/archive for the Local Communications Server is a combination of RAID for operational data, and the ECS Data Server archival of long-term mission data. The data storage/archive will have the capacity to meet CSMS requirements.

C-HRD-22300 The Local Communications Server data storage shall be compatible with POSIX compliant operating systems from several vendors.

C-HRD-22310 The Local Communications Server short-term data storage shall be compatible with the Enterprise Communications Server intermediate-term data storage.

C-HRD-22315 The Local Communications Server data storage shall support RAID level-5: striping with interleaved parity.

C-HRD-22320 The Local Communications Server data storage shall have the following hot swappable components:

a. Disks

b. Power Supplies

c. Fans

d. Disk-array controllers

C-HRD-22325 The Local Communications Server data storage shall be cross-strapped with the Local Management Server short-term data storage in supporting the CSMS requirements.

C-HRD-22335 The Local Communications Server data storage shall be capable of archiving data to the ECS Data Server archive.

C-HRD-22345 The Local Communications Server data archive shall adhere to ECS Data Server archival requirements for data storage and retrieval.

4.2.2.2.3 Peripherals

4.2.2.2.3.1 Local Disk Drives

The Local Communications Server disk drives will have the capacity to meet Local Communications Server operational requirements for report generation and system analysis.

C-HRD-22505 The Local Communications Server peripheral disk drives shall be capable of retrieving data stored from both the Local Communications server data storage and data archive.

4.2.2.2.3.2 Local Tape Drive

Local Communications Server tape drives will support Local Communications Server data storage and retrieval requirements.

C-HRD-22530 The Local Communications Server peripherals shall support at least one tape drive.

C-HRD-22535 The Local Communications Server peripheral tape drive shall have the following characteristics:

a. 4mm Digital Audio Tape format

b. Accept industry standard magnetic 4mm DAT (i.e. DDS-90)

c. Data transfer rate of 200KB/sec

C-HRD-22540 The Local Communications Server tape drives shall be upgradeable/replaceable within the same product family.

4.2.2.2.3.3 Local CD-ROM Drive

Local Communications Server CD-ROM drives will support Local Communications Server system software installation and retrieval requirements.

C-HRD-22565 The Local Communications Server peripherals shall support at least one CD-ROM drive.

C-HRD-22570 The Local Communications Server peripheral CD-ROM drive shall have the following characteristic:

a. Accept 600MB Compact Disk

C-HRD-22575 The Local Communications Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.

4.2.2.2.4 Hardware Cabinet

It is desirable, but not mandatory, for the Local Communications Server to be housed within one or more standard 19-inch width electronic equipment cabinets. The use of cabinets is an implementation issue dependent on available space at the SMC, DAACs, and EOC; and cost considerations. It is acknowledged that certain vendor platform costs may increase substantially if 19-inch mounting cabinets are made a requirement for procurement. The following are a list of desirable features for the CSS-DCHCI Local Communications Server hardware. In lieu of equipment cabinets, installation of hardware should adhere to site-specific installation procedures and considerations for power, grounding, and ventilation.

1. The Local Communications Server hardware cabinet should house the Local Communications Server processor, data storage, and peripherals.
2. The Local Communications Server hardware cabinet should provide a RETMA standard 19 inches of equipment mounting width.
3. The Local Communications Server hardware cabinet should be a minimum of 54" and a maximum of 72" tall, with standard 19" rack mounts.
4. The Local Communications Server hardware cabinet should provide a minimum of 24 inches of equipment mounting depth.
5. The Local Communications Server hardware cabinet should accommodate EIA Universal Standard RS-310 hole spacing or provide for a continuously adjustable equipment and panel mounting system.
6. The Local Communications Server hardware cabinet should provide removable side panels and rear door.
7. The Local Communications Server hardware cabinet should provide earth continuity for all components within.
8. The Local Communications Server hardware cabinet should provide sufficient equipment ventilation.
9. The Local Communications Server hardware cabinet should supply a minimum of one power controller.

4.2.2.3 Bulletin Board Server

The Bulletin Board Server will provide processors and peripheral equipment necessary for enabling user community access to ECS as required by the CSMS system design. The Bulletin Board Server will be standalone, and will coordinate with the Enterprise Communications Server to prevent a single point of failure for user community access to directory data. Client software and toolkits will be made available via the Bulletin Board Server, with backups of the software/toolkit safestored in the ECS data server archive.

C-HRD-23000 The Bulletin Board Server shall share data with the Enterprise Communications Server in supporting the CSMS requirements.

C-HRD-23005 The Bulletin Board Server shall preserve DAAC autonomy of operations and aggregate all ECS DAAC authentication/authorization policies by user

type and DAAC, to provide a integrated view of ECS for user registration, account administration, and authentication/authorization to ECS services.

C-HRD-23010 The Bulletin Board Server shall host the CSS software configuration items to create a single, secure unified access to all ECS services.

C-HRD-23015 The Bulletin Board Server shall host ECS client software and toolkits for ECS-external distribution.

4.2.2.3.1 Processor

C-HRD-23100 The Bulletin Board Server processor shall include a dedicated terminal to be used as a local systems operations console.

C-HRD-23105 The Bulletin Board Server processor shall be upgradeable/expandable with additional quantities and types of peripherals.

C-HRD-23110 The Bulletin Board Server processor shall be upgradeable/replaceable within the same product family without the need for any perturbation of any software or replacement of any peripheral or attached component.

C-HRD-23115 The Bulletin Board Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).

C-HRD-23120 The Bulletin Board Server processor terminal shall be compatible with the Management Workstation display device.

4.2.2.3.2 Data Storage/Archive

Data storage for the Bulletin Board Server is a combination of RAID for operational and software/toolkit data, and ECS data server archival of long-term mission data and safestore of ECS software and toolkits. The data storage will have the capacity to meet CSMS requirements.

C-HRD-23300 The Bulletin Board Server data storage shall be compatible with POSIX compliant operating systems from several vendors.

C-HRD-23310 The Bulletin Board Server data storage shall be capable of archiving data to the ECS data server archive for long-term storage and software/toolkit safestore.

C-HRD-23320 The Bulletin Board Server data archive shall adhere to ECS data server archival requirements for data storage and retrieval.

4.2.2.3.3 Peripherals

4.2.2.3.3.1 Local Tape Drive

Bulletin Board Server tape drives will support Bulletin Board Server data storage and retrieval requirements.

C-HRD-23530 The Bulletin Board Server peripherals shall support at least one tape drive.

C-HRD-23535 The Bulletin Board Server peripheral tape drive shall have the following characteristics:

a. 4mm Digital Audio Tape format

b. Accept industry standard magnetic 4mm DAT (i.e. DDS-90)

c. Data transfer rate of 200KB/sec

C-HRD-23540 The Bulletin Board Server tape drives shall be upgradeable/replaceable within the same product family.

4.2.2.3.3.2 Local CD-ROM Drive

Bulletin Board Server CD-ROM drives will support Bulletin Board Server system software installation and retrieval requirements.

C-HRD-23565 The Bulletin Board Server peripherals shall support at least one CD-ROM drive.

C-HRD-23570 The Bulletin Board Server peripheral CD-ROM drive shall have the following characteristic:

a. Accept 600MB Compact Disk

C-HRD-23575 The Bulletin Board Server peripheral CD-ROM drives shall be upgradeable/replaceable within the same product family.

4.2.2.3.4 Hardware Cabinet

It is desirable, but not mandatory, for the Bulletin Board Server to be housed within one or more standard 19-inch width electronic equipment cabinets. The use of cabinets is an implementation issue dependent on available space at GSFC; and cost considerations. It is acknowledged that certain vendor platform costs may increase substantially if 19-inch mounting cabinets are made a requirement for procurement. The following are a list of desirable features for the CSS-DCHCI Bulletin Board Server hardware. In lieu of equipment cabinets, installation of hardware should adhere to site-specific installation procedures and considerations for power, grounding, and ventilation.

1. The Bulletin Board Server hardware cabinet should house the Bulletin Board Server processor, data storage, and peripherals.
2. The Bulletin Board Server hardware cabinet should provide a RETMA standard 19 inches of equipment mounting width.
3. The Bulletin Board Server hardware cabinet should be a minimum of 54" and a maximum of 72" tall, with standard 19" rack mounts.
4. The Bulletin Board Server hardware cabinet should provide a minimum of 24 inches of equipment mounting depth.

5. The Bulletin Board Server hardware cabinet should accommodate EIA Universal Standard RS-310 hole spacing or provide for a continuously adjustable equipment and panel mounting system.
6. The Bulletin Board Server hardware cabinet should provide removable side panels and rear door.
7. The Bulletin Board Server hardware cabinet should provide earth continuity for all components within.
8. The Bulletin Board Server hardware cabinet should provide sufficient equipment ventilation.
9. The Bulletin Board Server hardware cabinet should supply a minimum of one power controller.

4.2.2.4 Terminal Access Server

The Terminal Access Server is allocated to release B and is not detailed in this version of the document. The Terminal Access Server provides modem and/or DSU/CSU access to ECS by users who are not network attached.

4.2.3 CSS-DCHCI Performance Requirements

C-HRD-26000	The Enterprise Communications Server shall be capable of 100 percent growth in Appendix A processing speed without modifications or upgrade to software.
C-HRD-26005	The Enterprise Communications Server shall be capable of 100 percent growth in Appendix A storage capacity without modifications or upgrade to software.
C-HRD-26010	The Local Communications Server shall be capable of 100 percent growth in Appendix A processing speed without modifications or upgrade to software.
C-HRD-26015	The Local Communications Server shall be capable of 100 percent growth in Appendix A storage capacity without modifications or upgrade to software.
C-HRD-26020	The Enterprise Communications Server shall be capable of meeting the capacity and performance characteristics of Appendix A.
C-HRD-26025	The Local Communications Server shall be capable of meeting the capacity and performance characteristics of Appendix A.
C-HRD-26030	The Bulletin Board Server shall be capable of meeting the capacity and performance characteristics of Appendix A.

4.2.4 CSS-DCHCI Security Requirements

C-HRD-27000 The CSS-DCHCI hardware selection criteria shall meet overall ECS security policies and system requirements.

C-HRD-27005 The CSS-DCHCI Bulletin Board Server shall provide a security perimeter for ECS

C-HRD-27010 The CSS-DCHCI Enterprise and Local Communications Servers shall be configured to provide autonomous DAAC security perimeters, FOS isolation, and an Iso-cell ECS security perimeter.

4.2.5 CSS-DCHCI RMA Requirements

C-HRD-28000 The CSS-DCHCI Enterprise Communications Server shall maintain one backup of all software and key data items in a separate physical location.

C-HRD-28005 The CSS-DCHCI Local Communications Server shall maintain one backup of all software and key data items in a separate physical location.

C-HRD-28010 The CSS-DCHCI functional string between the Enterprise Communications Server and the Local Communications Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).

C-HRD-28015 The CSS-DCHCI functional string between the Local Communications Server and ECS clients to the Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).

C-HRD-28020 The CSS DCHCI Enterprise Communications Server shall provide a function Ao of .998 (.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Enterprise Monitoring Server.

C-HRD-28025 The CSS-DCHCI Enterprise Communications Server functions not integral to providing backup functionality to the Enterprise Monitoring Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).

C-HRD-28030 The CSS DCHCI Local Communications Server shall provide a function Ao of .998 (.999998 design goal) and an MDT of 20 minutes (design goal of 5 minutes) for all functions integral to providing a backup to the Local Management Server.

C-HRD-28035 The CSS-DCHCI Local Communications Server functions not integral to providing backup functionality to the Local Management Server shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).

C-HRD-28040 The CSS-DCHCI Bulletin Board Server functions shall provide a function Ao of 0.96 (.998 design goal) and an MDT of four hours (1.5 hour design goal).

4.2.6 CSS-DCHCI Evolvability Requirements

There are no L3 evolvability requirements directly allocated to CSS hardware.

4.3 ISS Internetworking Hardware Configuration Item

4.3.1 Overview of ISS-INHCI

The ISS Internetworking Hardware CI (ISS-INHCI) is the hardware to host all ISS software described in section 8. The ISS-INHCI logically includes routers, hubs, switches, and LAN analyzers, and plant cabling components. Unique configurations of these components of the ISS-INHCI exist for the GSFC LAN, EDC LAN, LaRC LAN, and MSFC LAN in IR-1; and the GSFC LAN, GSFC EOC LAN, EDC LAN, LaRC LAN and MSFC LAN in R-A..

4.3.2 ISS-INHCI Functional Requirements

4.3.2.1 ISS Release A LANs

C-HRD-31000 The ISS shall provide LANs at the following Release A sites:

a. GSFC DAAC LAN

b. GSFC EOC LAN

c. EDC DAAC LAN

d. LaRC DAAC LAN

e. MSFC DAAC LAN

f. GSFC SMC LAN

4.3.2.2 ISS Components

C-HRD-32000 The ISS shall use physical devices and Medium Access Control protocols compatible with the following standards:

a. IEEE 802.2 (Logical Link Control)

b. IEEE 802.3 (MAC for Ethernet)

c. IEEE 802.6 (MAC for SMDS)

d. ANSI X3T9.5 (MAC for FDDI).

C-HRD-32010 The ISS physical components, and services shall have the capability to be monitored via SNMP agents.

4.3.2.3 LAN Analysis Equipment

The LAN Analysis Equipment will provide equipment for monitoring network performance, operation, checkout, and test.

C-HRD-34000 The LAN Analysis Equipment shall provide protocol analysis through the transport layer for all ISS LAN protocols and interconnection protocols to MANs/WANs.

C-HRD-34010 The LAN Analysis Equipment shall include:

a. Communications line monitors to store and display up to 10,000 bytes of data sent and received over any of the communications lines at rates of 10MB/sec to 100MB/sec, and supporting the protocols used within and interconnecting ECS.

b. Digital VOM/multimeters

c. Local Area Network analyzers

4.3.3 ISS-INHCI Performance Requirements

All end-to-end system, SDPS, and FOS requirements that cross a network place a requirement on the performance of the network.

C-HRD-36000 The EOC LAN loop delay contribution shall not exceed more than 500 msec (goal 250 msec) seconds of the total ECS delay of 2.5 seconds for emergency real-time commands.

C-HRD-36010 The EOC Operational LAN backbone shall be able to support a peak traffic rate of 24 Mbps to support AM-1 flows from the Ecom interface.

C-HRD-36020 The ISS shall provide wide area bandwidth necessary to support data transfer in accordance with Release A requirements specified in "Communications Requirements for the ECS Project", 194-220-SE3-001.

C-HRD-36030 The ISS shall provide sufficient local area network bandwidth at the LaRC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS in accordance with the Release A network I/O sizing listed in Appendix A..

C-HRD-36040 The ISS shall provide sufficient local area network bandwidth at the MSFC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS in accordance with the Release A network I/O sizing listed in Appendix A.

C-HRD-36050 The ISS shall provide sufficient local area network bandwidth at the GSFC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS in accordance with the Release A network I/O sizing listed in Appendix A.

C-HRD-36060 The ISS shall provide sufficient local area network bandwidth at the EDC DAAC to support data transfer between and among physical nodes provided by SDPS, MSS and CSS in accordance with the Release A network sizing listed in Appendix A.

C-HRD-36065 The ISS shall reuse the existing V0 DAAC LAN at EDC for Release A.

C-HRD-36070 The ISS LANs at the GSFC, MSFC and LaRC DAAC sites shall be capable of supporting twice the R-A network traffic load estimates without redesign.

C-HRD-36080 The ISS LANs at the Release-A DAAC sites shall be designed in a manner that allows

a. Nodes to be added to any given LAN segment.

b. Additional LAN segments to be added to the LAN.

C-HRD-36090 The EOC Operational LAN shall be able to support 230 network devices without redesign.

C-HRD-36100 The EOC Operational LAN shall be able to support peak data rates of up to 48 Mbps without redesign.

4.3.4 ISS-INHCI Security Requirements

C-HRD-37000 The ISS networks shall support the use of network and transport layer filtering to control access from internal and external interfaces

4.3.5 ISS-INHCI RMA Requirements

The ISS RMA requirements are documented in section 7.1.3, 'RMA Requirements'.

4.3.6 ISS-INHCI Evolvability Requirements

C-HRD-39000 The ISS-INHCI DAAC LANs shall provide transparent portability across heterogeneous site LAN architectures.

C-HRD-39005 The ISS-INHCI DAAC LANs shall enable expansion to GByte networks including the ability to provide increased volume of data distribution and access.

4.4 Facility Requirements

4.4.1 EDF

4.4.1.1 EMC

C-HRD-41000 The EDF in the IR-1 timeframe shall provide a Enterprise Monitoring Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Enterprise Communications Server

C-HRD-41005 The EDF in the IR-1 timeframe shall provide a Enterprise Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Enterprise Monitoring Server

C-HRD-41010 The EDF in the IR-1 timeframe shall provide a Bulletin Board Server configured with:

a. One Tape Drive

b. One CD-ROM Drive

C-HRD-41015 The EDF in the IR-1 timeframe shall provide two (2) Data Storage Unit supporting RAID level 5, one for the shared Enterprise Monitoring/Enterprise Communications, and the other for the Bulletin Board Server.

C-HRD-41020 The EDF in the IR-1 timeframe shall provide four (4) Management Workstations, which can perform any EMC function.

C-HRD-41025 The EDF in the IR-1 timeframe shall provide 1 system printer.

4.4.1.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at the EDF.

C-HRD-41500 The EDF in the IR-1 timeframe infrastructure shall provide one EDF LAN.

4.4.2 GSFC

4.4.2.1 LSM

C-HRD-42000 The GSFC LSM in the IR-1 timeframe shall provide a Local Management Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

C-HRD-42005 The GSFC LSM in the R-A timeframe shall provide a Local Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Management Server

C-HRD-42010 The GSFC LSM in the R-A timeframe shall provide one Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.

C-HRD-42015 The GSFC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.

C-HRD-42020 The GSFC LSM in the R-A timeframe shall provide 1 system printer.

4.4.2.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at GSFC.

C-HRD-42500 The GSFC infrastructure in the R-A timeframe shall provide one GSFC LAN.

4.4.2.3 EMC

C-HRD-42700 The GSFC EMC in the R-A timeframe shall provide an enterprise monitoring server, enterprise communications server, four (4) Management Workstations, one (1) printer, and bulletin board server transferred from the IR-1 EDF.

C-HRD-42705 The GSFC EMC in the R-A timeframe shall provide, via the ECS data server, a Enterprise Monitoring Server long-term data storage capability.

4.4.3 EOC

4.4.3.1 LSM

C-HRD-43000 The EOC LSM in the R-A timeframe shall provide a Local Management Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Communications Server

C-HRD-43005 The EOC LSM in the R-A timeframe shall provide a Local Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Management Server

C-HRD-43010 The EOC LSM in the R-A timeframe shall provide one Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.

C-HRD-43015 The EOC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.

C-HRD-43020 The EOC LSM in the R-A timeframe shall provide 1 system printer.

4.4.3.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at the EOC.

C-HRD-43500 The EOC infrastructure in the R-A timeframe shall provide one EOC LAN.

4.4.4 MSFC

4.4.4.1 LSM

C-HRD-44000 The MSFC LSM in the IR-1 timeframe shall provide a Local Management Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

C-HRD-44005 The MSFC LSM in the R-A timeframe shall provide a Local Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Management Server

C-HRD-44010 The MSFC LSM in the R-A timeframe shall provide one Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.

C-HRD-44015 The MSFC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.

C-HRD-44020 The MSFC LSM in the R-A timeframe shall provide 1 system printer.

4.4.4.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at MSFC.

C-HRD-44500 The MSFC infrastructure in the R-A timeframe shall provide one MSFC LAN.

4.4.5 LaRC

4.4.5.1 LSM

C-HRD-45000 The LaRC LSM in the IR-1 timeframe shall provide a Local Management Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

C-HRD-45005 The LaRC LSM in the R-A timeframe shall provide a Local Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Management Server

C-HRD-45010 The LaRC LSM in the R-A timeframe shall provide one Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.

C-HRD-45015 The LaRC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.

C-HRD-45020 The LaRC LSM in the R-A timeframe shall provide 1 system printer.

4.4.5.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at LaRC.

C-HRD-45500 The LaRC infrastructure in the R-A timeframe shall provide one LaRC LAN.

4.4.6 EDC

4.4.6.1 LSM

C-HRD-46000 The EDC LSM in the IR-1 timeframe shall provide a Local Management Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

C-HRD-46005 The EDC LSM in the R-A timeframe shall provide a Local Communications Server configured with:

a. Two Fixed Disks

b. One Tape Drive

c. One CD-ROM Drive

d. Storage cross-strapped with Local Management Server

C-HRD-46010 The EDC LSM in the R-A timeframe shall provide one Data Storage Unit supporting RAID level 5 cross strapped between the local management and local communications servers.

C-HRD-46015 The EDC LSM in the R-A timeframe shall provide two (2) Management Workstations, which can perform any EOC LSM function.

C-HRD-46020 The EDC LSM in the R-A timeframe shall provide 1 system printer.

4.4.6.2 Infrastructure

A local area network will be provided to support communications between the Computing platforms at EDC.

C-HRD-46500 The EDC infrastructure in the R-A timeframe shall provide one EDC LAN.

This page intentionally left blank.

5. MSS Functional Requirements

Section 5 contains the functional requirements associated with the System Management Subsystem (MSS). This includes the Management Application Services, Common Management Services and Management Agent Services. This section is organized by configuration items as follows:

5.1 General Requirements

5.2 Management Software Configuration Item (MCI)

5.3 Management Logistics Configuration Item (MLCI)

5.4 Management Agent Configuration Items (MACI).

As shown in Table 5-1, the MSS configuration items (CIs) have change since the system design review. The System Management Configuration Item (SMCI) and the Network Management Configuration Item (NMCI) have been combined into the Management Software Configuration Item (MCI). This provides enterprise management of all ECS resources (network, system and applications) within a domain. Most MSS services reside primarily in one CI, however services in other CIs may provide direct support to management application services. Report generation services are provide by the Database Management System (DBMS) and other management application services as provide by COTS for Interim Release 1 and Release A. Policies and procedures services are provided by Office Automation tools for Interim Release 1 and Release A

Table 5-1. Management Application to CI Mapping

Service \ CI	MCI	MLCI	MACI
Fault Management	P		S
Performance Mgt	P		S
Security Management	P		
Accountability Mgt	P		
Configuration Mgt	P	P	
Management Agent	S		P

P-Primary S-Support

5.1 General Requirements

5.1.1 MSS Interface Requirements

The MSS interfaces are identified in the following Figure 5.1-1.

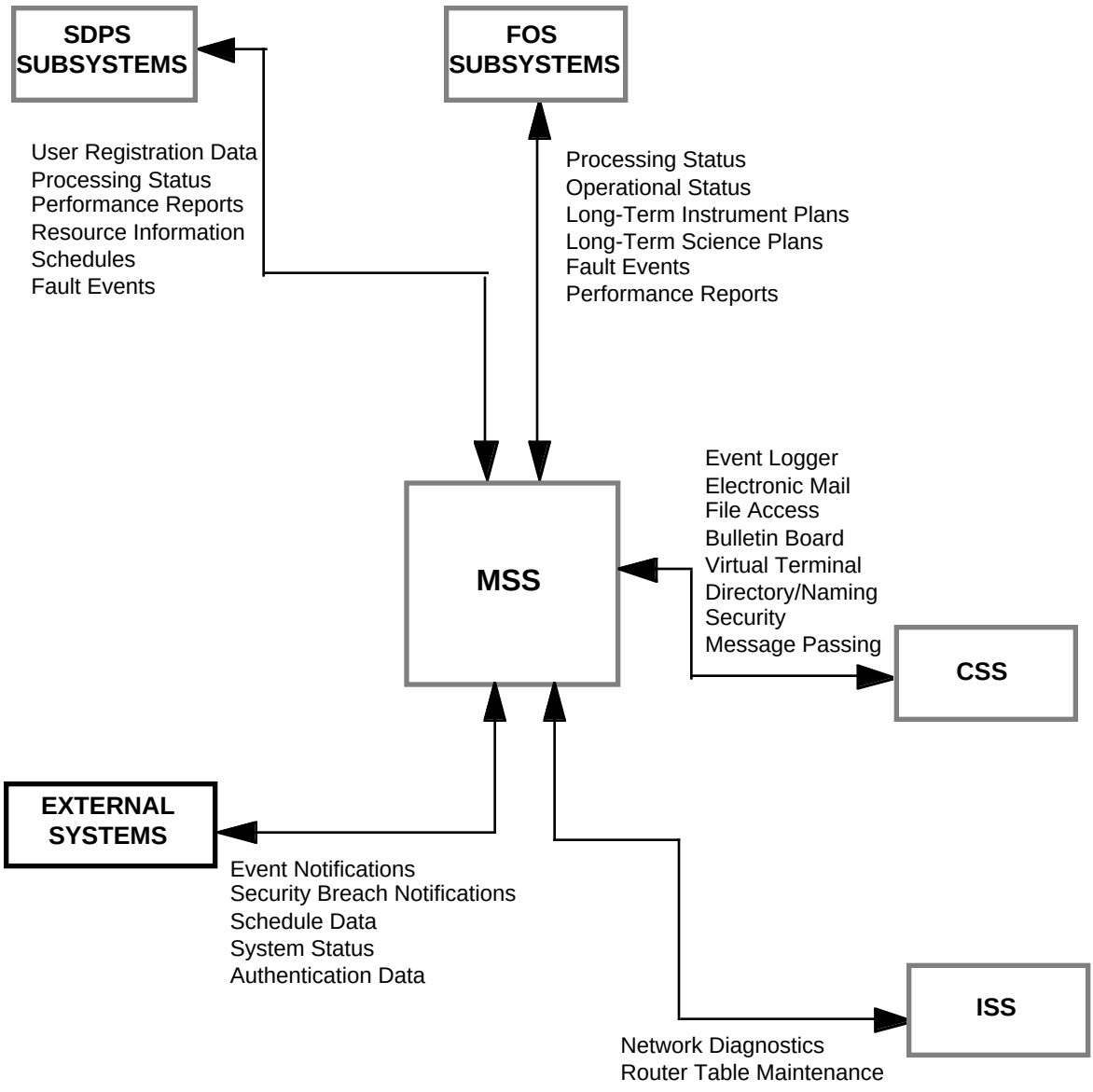

Figure 5.1-1 MSS Interface Diagram

5.1.1.1 MSS/External Interface Requirements

Table 5.1-1 summarizes the MSS external interfaces and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-1. MSS/External Interface (1 of 2)

Source	Destination	Data Description
MSS	Ecom	Schedule data Authentication data Security breach notification
Ecom	MSS	Ecom Status Authentication data Security breach notification
MSS	V0	Schedule data Authentication data Setup data
V0	MSS	Authentication data Setup data Security audit trail
MSS	NCC (NISS)	Security breach notification Scheduling data
NCC (NISS)	MSS	Event Notifications Fault Status Down Time Summary
MSS	NOLAN (NISS)	Security breach notification
NOLAN (NISS)	MSS	Link utilization & network perf Event notifications Fault status Estimated down time Fault summary Security breach notification
MSS	ADC(NOAA)	Network Management Information Advertising Info Authentication data Guide Queries Browse Data Product delivery status request Product delivery status
ADC(NOAA)	MSS	Network Management Information Authentication data Product delivery status request Product delivery status
MSS	ODC	Schedule data
MSS	TRMM	Schedule data
TRMM	MSS	Schedule data

Table 5.1-1. MSS/External Interface (2 of 2)

Source	Destination	Data Description
SCF	MSS	Security audit trail Security breach notification
MSS	LANDSAT 7	System management status
LANDSAT 7	MSS	Resource utilization costs System management status
MSS	NSI	Security breach notification
NSI	MSS	Event notification Fault analysis status Fault resolution Network & link status Security breach notification
MSS	PSCN	Security breach notification
PSCN	MSS	Fault notification Fault analysis status Fault resolution Security breach notification
MSS	EDOS	Authentication data Schedule data Security breach notification
EDOS	MSS	Authentication Data Schedule data Security breach notification
MSS	IP	Schedule data Configuration mgt data Network management data Security breach notification Product delivery status request Product delivery status
IP	MSS	Authentication Data Network management data Product delivery status request Product delivery status Security breach notification Schedule data

The external interface requirements for the MSS are:

C-MSS-10010 The MSS shall interface with the Ecom systems to exchange data identified in Table 5.1-1 as specified in the ECS/Ecom IRD.

C-MSS-10020 The MSS shall interface with the Version 0 system to exchange data identified in Table 5.1-1 as specified in the ECS/V0 IRD, 194-219-SE1-004.

C-MSS-10030 The MSS shall interface with the Science Computing Facility (SCF) to exchange data identified in Table 5.1-1 as specified in ECS/SCF IRD, 194-219-SE1-005.

C-MSS-10040 The MSS shall interface with the NASA Institutional Support System (NISS) to exchange data identified in Table 5.1-1 as specified in ECS/NISS IRD, 194-219-SE1-020.

C-MSS-10050 The MSS shall interface with the Affiliated Data Centers (ADC) to exchange data identified in Table 5.1-1 as specified in ECS/ADC IRD, 219-CD-006.

C-MSS-10060 The MSS shall interface with the Tropical Rainfall Measuring Mission (TRMM) to exchange data identified in Table 5.1-1 as specified in ECS/TRMM IRD, 194-219-SE1-018.

C-MSS-10070 The MSS shall interface with the Landsat 7 System to exchange data identified in Table 5.1-1 as specified in ECS/Landsat 7 IRD, 219-CD-003.

C-MSS-10080 The MSS shall interface with the NASA Science Internet (NSI) to exchange data identified in Table 5.1-1 as specified in ECS/NSI IRD, 194-219-SE1-001.

C-MSS-10090 The MSS shall interface with the Program Support Communications Network (PSCN) to exchange data identified in Table 5.1-1 as specified in ECS/PSCN IRD, 193-219-SE1-008.

C-MSS-10100 The MSS shall interface with the EDOS to exchange data identified in Table 5.1-1 as specified in EDOS/EGS IRD, 560-EDOS-0211.

C-MSS-10110 The MSS shall interface with the International Partners (IP) for Data Interoperability to exchange data identified in Table 5.1-1 as specified in ECS/IP IRD, 194-219-SE1-015.

5.1.1.2 MSS/SDPS Interface Requirements

Table 5.1-2 summarizes the MSS interface with the SDPS subsystem and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-2. MSS/SDPS Subsystem Interface

Source	Destination	Data Description
MSS	All SDPS subsystems	Accountability data User registration data Performance reports Resource info Schedules
All SDPS subsystems	MSS	Fault data Performance reports Schedules
MSS	Client	User registration Product delivery status
Client	MSS	Client status User-Request product status
Ingest	MSS	Ingest status Ingest log
Data Server	MSS	Data Server log Data Server status
Data Processing	MSS	Processing info Processing status Product generation data

The MSS interface requirement with the SDPS subsystem follows:

C-MSS-10200 The MSS shall interface with the SDPS subsystems to exchange the data items in Table 5.1-2 as specified in the ECS internal ICDs, 313-DV3-003.

5.1.1.3 MSS/FOS Interface Requirements

Table 5.1-3 summarizes the MSS interface with the FOS subsystem and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-3. MSS/FOS Subsystem Interface

Source	Destination	Data Description
MSS	Planning & Sched	Long-Term Instrument Plans (LTIP) Long-Term Science Plans (LTSP)
Planning & Sched	MSS	P&S management status information P&S operational status information
Command	MSS	Command management status information Command operational status information
Analysis	MSS	Analysis management status information Analysis operational status information
Command Management	MSS	Cmd mgt management status information Cmd mgt operational status information

The MSS interface requirement with the FOS subsystem at another site follows:

C-MSS-10300 The MSS shall interface with the FOS subsystems to exchange the data items in Table 5.1-3 as specified in the ECS internal ICDs, 313-DV3-003.

5.1.1.4 MSS/MSS Interface Requirements

Table 5.1-4 summarizes the MSS interface between LSM at sites and EMC at the SMC, and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-4. MSS/MSS Subsystem Interface

Source	Destination	Data Description
LSM	EMC	History log summary data Security events Fault events Performance events SDPS product generation data Registration data
EMC	LSM	Data requests Policy directives Software distribution Registration data
LSM	LSM	Security events Fault events Performance events SDPS product generation data Registration data

The MSS interface requirement with the MSS subsystem at an other site follows:

C-MSS-10400 The MSS at a site shall interface with the MSS subsystems at the SMC and other sites to exchange management data items in Table 5.1-4.

5.1.1.5 MSS/CSS Interface Requirements

Table 5.1-5 summarizes the MSS interface with the CSS subsystem and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-5. MSS/CSS Subsystem Interface

Source	Destination	Data Description
CSS API	MSS	Event logger Time Message Passing
CSS server	MSS	Electronic Mail File Access Bulletin Board Virtual Terminal Directory/Naming Security
MSS	CSS server	Service request

The MSS interface requirement with the CSS subsystem follows:

C-MSS-10410 The MSS shall interface with the CSS subsystems to exchange the data items in Table 5.1-5 as specified in the ECS internal ICDs, 313-DV3-003.

5.1.1.6 MSS/ISS Interface Requirements

Table 5.1-6 summarizes the MSS interface with the ISS subsystem and includes the source and destination of the interface, and a brief description of the data item.

Table 5.1-6. MSS/ISS Subsystem Interface

Source	Destination	Data Description
MSS	ISS	Request network protocol status Request network hardware status Network protocol diagnostic Network hardware diagnostic Router table maintenance
ISS	MSS	Network protocol status data Network hardware status data

The MSS interface requirement with the ISS subsystem follows:

C-MSS-10420 The MSS shall interface with the ISS subsystems to exchange the data items in Table 5.1-6 as specified in the ECS internal ICDs, 313-DV3-003.

5.1.2 MSS Performance Requirements

C-MSS-00200 The MSS services shall allocate 10% of development resources for IV&V activity.

5.1.3 MSS RMA Requirements

C-MSS-00010 The MSS services shall have an operational availability of .998 and an MDT of 20 minutes or less for critical services.

C-MSS-00020 The MSS services shall have no single point of failure for functions associated with network databases and configuration data.

C-MSS-00030 The MSS services shall be extensible in its design to provide capability for growth and enhancement.

5.1.4 MSS Evolvability Requirements

The MSS evolvability requirements are allocated to each MSS service class and are addressed in each appropriate section.

5.2 Management Software Configuration Item (MCI)

5.2.1 Common Management Services

The Common Management Service provides the underlying common management services that form the foundation for the integration of management applications. These common management services comprise the management framework upon which system management application are built and promotes interoperabilty among management applications. All of the common management services requirements will be provided for the Interim Release 1 (IR-1). The Common Management Service is a collection of the following set of services:

Monitor/Control

Discovery

Maps/Collection

Management User Interface

Management Data Access

Database Management System (DBMS)

A context diagram for Common Management Services is provide in Figure 5.2-1.

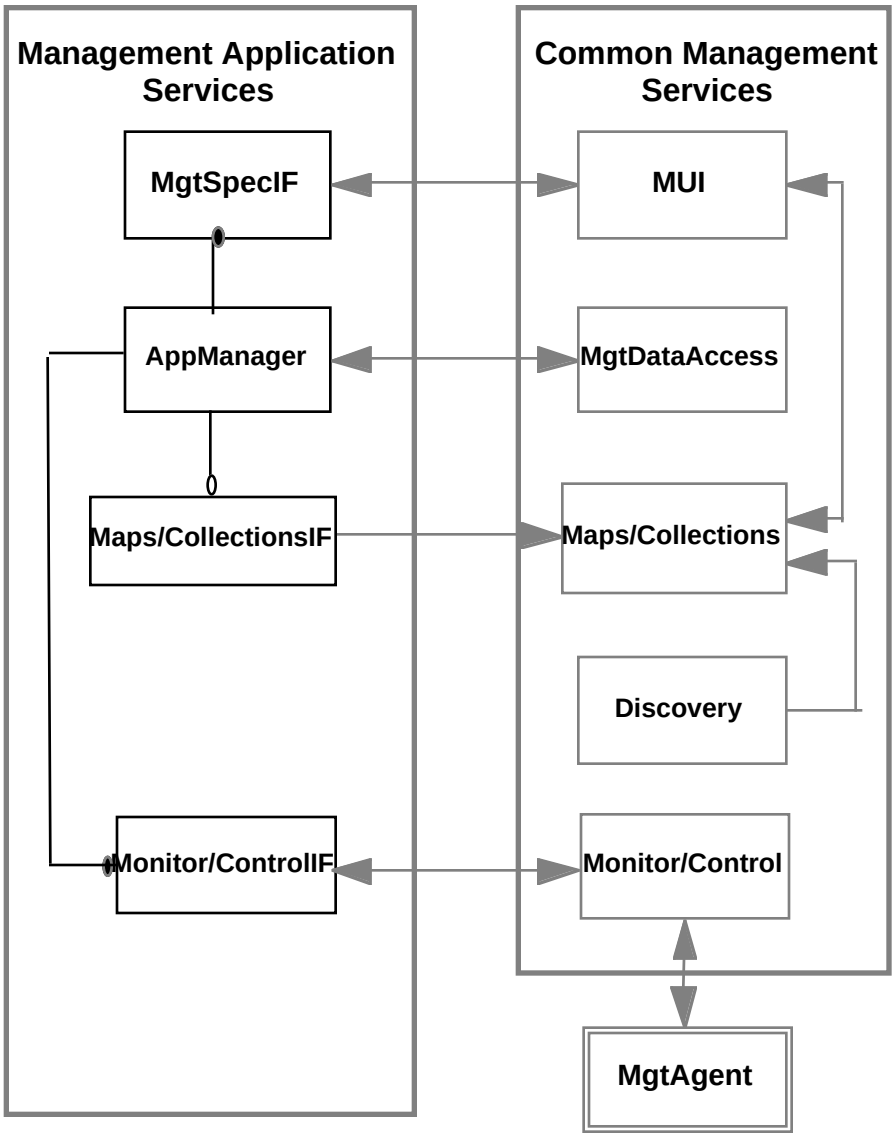

Figure 5.2-1. CMS Context Diagram

5.2.1.1 Monitor/Control Service

5.2.1.1.1 Overview Monitor/Control Service

The Monitor/Control Service provides a uniform means for management applications to monitor and control managed objects, request and receive status on managed objects and process events/traps from managed objects. This service provides the infrastructure via Simple Network Management Protocol (SNMP) for system management applications to control the collection and monitoring of managed objects attributes that are defined in the Management Information Base (MIB); and the event management capabilities to support receiving, reporting, disseminating, logging of system event and for triggering actions in response to system events.

5.2.1.1.2 Monitor/Control Service Functional Requirements

C-MSS-16005 The ECS management protocol shall be the SNMP standard as specified in RFC 1157.

C-MSS-16010 MSS Monitor/Control Service shall communicate via ECS management protocol with the Management Agent Service in test or operational mode.

C-MSS-16020 The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to request management data on a managed object.

C-MSS-16030 The MSS Monitor/Control Service shall be able to communicate via ECS management protocol with the MSS Management Agent Service to send ECS management set messages to configure and control the processing performed by the ECS management agent.

C-MSS-16040 The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to receive ECS management traps/events.

C-MSS-16050 The MSS Monitor/Control Service shall allow customized M&O Staff-event notifications and automatic actions.

Note: This capability will allow the network-event message to be tailorable as to what text and MIB variables are represented in a network-event message.

C-MSS-16060 The MSS Monitor/Control Service shall allow the capability to set thresholds on managed resources that are monitored.

C-MSS-16070 The MSS Monitor/Control Service shall automatically report when a threshold has been exceeded by generating a ECS management event.

C-MSS-16100 The MSS Monitor/Control Service shall perform the following protocol test on managed network nodes:

a. IP test

b. TCP test

c. SNMP test

d. UDP test

e. ICMP test

5.2.1.2 Discovery Service

5.2.1.2.1 Overview Discovery Service

The discovery service provides the basis for managed resource identification and detection (such as a repaired router returning to service). It provides a capability to keep track of the system configuration by providing a common set of rules and interfaces to:

- register and unregistered new objects
- store information about them (e.g. in maps, collections etc.)
- notify M&O specialist about discovery instances.

5.2.1.2.2 Discovery Service Functional Requirements

C-MSS-20010 The MSS Discovery Service shall discover (via network protocol) new instances of managed objects.

Note: Managed objects include network devices and host computers in IR-1.

C-MSS-20020 The MSS Discovery Service shall detect missing occurrences of managed objects.

C-MSS-20030 The MSS Discovery Service shall report missing occurrences of managed objects.

C-MSS-20040 The MSS Discovery Service shall update the object database after the Discovery Service receives a request to register/unregister a managed object.

5.2.1.3 Maps/Collection Service

5.2.1.3.1 Overview Maps/Collection Service

The uniform management of the relationships between managed objects and the collection of objects in a maps and sub-maps is provided by the Maps/Collections service. This service manages the collection-object and map-object relationships. The collection-object relationship provides the basic capability to manage unordered sets of references to other objects. The map-object relationship, in addition to maintaining the object references, maintains a graph to describes the connection between individual members of the map.

5.2.1.3.2 Maps/Collection Service Functional Requirements

C-MSS-14010 The MSS Maps/Collection Service shall retain the status of managed objects and their relationship to symbols that comprise a graphical representation of the physical network topology.

C-MSS-14020 The MSS Map/Collection Service shall provide a capability to define maps and objects.

C-MSS-14030 The MSS Map/Collection Service shall provide a capability to define a hierarchical relationship between maps and sub-maps (i.e., a graphical hierarchical tree)

C-MSS-14040 The MSS Map/Collection Service shall propagate events associated with objects up the hierarchical tree

5.2.1.4 Management User Interface (MUI) Service

5.2.1.4.1 Overview MUI Service

The management user interface provides tools and services needed to build user interfaces for distributed Object Oriented applications in a technology independent way. Important features of the MUI are the ability to present management information maps, to support dialog interaction, and to separate presentation from interaction. For example, applications post the presentation information to the MUI which in turn maps this information to a specific toolkit like Motif. This will allow the application to remain independent of the underlying toolkit.

5.2.1.4.2 MUI Service Functional Requirements

C-MSS-12005	The MSS Management User Interface (MUI) Service shall be compatible with the ECS management framework.
C-MSS-12010	The MSS Management User Interface (MUI) Service shall provide a graphical user interface that is OSF/MOTIF compliant
C-MSS-12020	The MSS MUI Service shall have the capability to respond to keyboard and mouse input devices
C-MSS-12030	The MSS MUI Service shall provide a capability for the M&O Staff to add/delete a symbol and to modify a symbol's shape, color and position
C-MSS-12040	The MSS MUI Service shall provide a capability for an application to add/delete a symbol and to modify a symbol's shape, color and position
C-MSS-12050	The MSS MUI Service shall provide a capability for the M&O Staff to add, delete, and modify text strings
C-MSS-12060	The MSS MUI Service shall provide a capability for an application to add, delete, and modify text strings
C-MSS-12070	The MSS MUI Service shall have the capability to provide options and methods to the M&O Staff for screen configuration changes (color, symbol placement, etc.) and for retaining the changes from session to session
C-MSS-12080	The MSS MUI Service shall provide a capability for an applications to alert the M&O Staff
C-MSS-12090	The MSS MUI Service shall provide a capability for an applications to establish a dialog session with the M&O Staff
C-MSS-12100	The MSS MUI Service shall provide a capability for the M&O Staff to load and unload vendor or ECS defined MIB
C-MSS-12110	The MSS MUI Service shall provide a capability for an applications to load and unload vendor or ECS defined MIB
C-MSS-12120	The MSS MUI Service shall provide a capability for the operator to browse MIB values
C-MSS-12130	The MSS MUI Service shall provide the capability for the M&O Staff to register and unregister managed objects.
C-MSS-12140	The MSS MUI Service shall provide the capability for an application to register and unregister managed objects. NOTE: Managed objects will include network devices and ECS host systems in IR-1

C-MSS-12170 The MSS MUI Service shall provide the capability to register and unregister management applications.

C-MSS-12180 The MSS MUI Service shall provide the capability for an application to display on-line help windows

5.2.1.5 Management Data Access Service

5.2.1.5.1 Overview Management Data Access Service

The Management Data Access Service provides the tools via application APIs for management applications to create, update and delete ECS management data. ECS management data includes all event log files, security and data audit trails, and the EMC and sites management database. All ECS management data will be maintained and accessed via this service.

The capabilities and functions of the management data access service are:

a. a scheduler to archive and load log files into a site and/or EMC management database

b. a capability to browse log files

c. a capability to selectively read management data

5.2.1.5.2 Management Data Access Service Functional Requirements

C-MSS-18040 The MSS Management Data Access Service shall maintain the integrity of the management database.

C-MSS-18050 The MSS Management Data Access Service's shall utilize CSS Services to access/transfer management data.

C-MSS-18060 The Management Data Access Service shall provide the capability for an application to access management data.

C-MSS-18070 The MSS Management Data Access Service shall provide the capability to selectively access management data.

C-MSS-18200 The MSS Management Data Access Service shall provide the capability for an application via APIs to update fields in the management database.

C-MSS-18220 The MSS Management Data Access Service shall provide the capability for an application via APIs to alter tables and fields in the management database.

C-MSS-18260 The MSS Management Data Access Service shall have the capability to schedule the transfer and loading log files into the management database at the site.

C-MSS-18270 The MSS Management Data Access Service shall have the capability to schedule the archiving of log files at the site.

C-MSS-18280 The MSS Management Data Access Service shall have the capability to schedule the transfer of management data at the sites to the SMC.

C-MSS-18330 The MSS Management Data Access Service shall provide the capability for an applications to append records to a log file

C-MSS-18340 The MSS Management Data Access Service shall provide the capability for an application to selectively read a record from a log file

C-MSS-18350 The MSS Management Data Access Service shall provide the capability for an application to load log files into the management database at the site

5.2.1.6 MSS Database Requirements

5.2.1.6.1 Overview Database Management System (DBMS)

A COTS Database Management System (DBMS) will be provided as a central repository for ECS management data. Additioanlly, a COTS report generation product will be integrated with the DBMS to support ad hoc statistical analysis and report generation based on management data stored in the database.

5.2.1.6.2 DBMS and ReportingFunctional Requirements

C-MSS-90020 The DBMS shall support a client-server design paradigm with distributed data allocation.

C-MSS-90030 The DBMS shall provide security access control based upon userid, role and privleges for the following:

a. database

b. database object

c. database operations

C-MSS-90060 The DBMS shall provide an SQL interface with query, update, and administrative functions capabilities.

C-MSS-90070 The DBMS shall be in compliance with the SQL-2 of Federal Information Processing System Publication (FIPS PUB) 127-1.

C-MSS-90080 The DBMS shall support mathematical operations to generate statistics from management data to include:

a. average

b. maximum

c. minimum

d. standard deviation

e. sum

f. count

g. variance

C-MSS-90120 The DBMS shall be compatible with the ECS management framework to support the import of the ECS management framework data.

C-MSS-90140 The DBMS shall support, or be accessed via, CSS session-establishment services.

C-MSS-90150 The DBMS shall support access structures (i.e., single-level indexes, multilevel indexes) to improve the efficiency of retrieval of management data.

C-MSS-90160 The DBMS shall support features in compliance with X/Open environment to include the following:

a. hardware independence

b. operating systems independence

c. network protocols independence

C-MSS-90170 The DBMS shall provide the following bulk data load capabilities:

a. direct writes from data files to database

b. loading of files containing fixed and variable length records

c. incremental bulk load

d. maintain indexes during data loads

C-MSS-90180 The DBMS shall provide the following database backup capabilities:

a. entire database

b. incremental data

c. operator specified database items

C-MSS-90190 The DBMS shall provide capabilities for specifying frequency, time and type of backups.

C-MSS-90200 The DBMS shall perform on-line disk management functions to include:

a. relocation of database files to different disks

b. expansion of database size by adding new physical data files to it on-line

c. dynamic pre-allocation of contiguous space for tables

d. database objects and indexes can span physical files

e. database objects and indexes can exist on different disks

C-MSS-90210 The DBMS shall support the following features:

a. data compression of nulls and variable length character strings, and indexes

b. space reclaimed from deleted records automatically

c. variable-length column storage

C-MSS-90230 The DBMS shall provide a transaction roll backward capability to a specified time or state:

a. restore a database

b. restore all or operator selected database objects of any database

C-MSS-90240 The DBMS shall provide for automatic database recovery including a means to:

a. automatically restore undamaged portions of a database and recover work in progress after a system or component failure

b. achieve dynamic backout of database modifications, performed by a failing transaction, that does not affect separate, concurrent tasks

C-MSS-90260 The DBMS shall provide a capability to export, archival, and restore a database.

C-MSS-90280 The DBMS shall provide the capability to issue and record a database checkpoint.

C-MSS-90290 The DBMS shall provide an audit trail of chronological activities in the database.

C-MSS-90500 The Report Generator shall be compatible with the DBMS.

C-MSS-90510 The Report Generator shall provide a Motif based Graphical User Interface (GUI) for creating ad hoc reports.

C-MSS-90520 The Report Generator shall have the capability to generate ad hoc reports from management data maintained in the DBMS.

C-MSS-90530 The Report Generator shall provide the capability to format reports to include the report:

a. title

b. header

c. footer

d. page number

e. date/time of report.

C-MSS-90570 The Report Generator shall have the capability to generate charts and graphs (e.g., bar, pie, line, etc.) from management data maintained in the DBMS.

C-MSS-90600 The Report Generator shall provide the capability to redirect generated reports to;

a. console

b. disk file

c. printer

5.2.1.7 MSS Office Automation Tools Requirements

5.2.1.7.1 Overview Office Automation (OA) Tools

COTS Office Automation (OA) tools will be provided, in the Interim 1 and Release A timeframe, for the M&O Staff to perform ECS policy and procedure services required for the specific release. OA tools, together with E-mail and Bulletin Board services, will support the flow down of policies and procedures from the SMC to the sites by the M&O Staff.

The OA tools provides a set of general purpose, integrated COTS software applications that can be used in support of other MSS services and M&O Staff functions. It provides the M&O staff the means to partially automate some of its ECS functional activities. The office automation capability will serve as an interim measure until function-specific automation is provided in accordance with the ECS Release Plan. OA tools include word processing, spreadsheet, and graphics management capabilities.

5.2.1.7.2 OA Tools Functional Requirements

C-MSS-91010 The MSS Office Automation word processing capability shall facilitate the:

a. preparation, revision, and recording of documents, messages, reports, and date

b. import, transformation, and editing of documents produced by other word processing packages

c. insertion of worksheet and graphic images into documents, messages, and reports

d. transfer of document, message, and report information to spreadsheet and graphics applications

e. printing of documents, messages, reports, and data

C-MSS-91020 The MSS Office Automation shall provide a spreadsheet capability that:

a. simulates and displays an accountant's worksheet

b. enables revisions and calculations on the displayed worksheet's data

c. enables transfer of the worksheet data to database, word processing and graphics applications

d. enables printing of worksheet information

C-MSS-91030 The MSS Office Automation shall provide a graphics capability that enables:

a. the development, modification, recording, and printing of graphic images

b. the transfer of graphics images to word processing documents, messages, and reports

5.2.2 Fault Management Application Service

Fault Management addresses the detection, isolation, diagnosis, and the recovery from a fault condition in a managed object, to the restoration of the affected system or service to an operational state. The Managed Objects in Release A for which Fault Management is provided include network devices, operating systems, peripheral devices, processes, applications (to include algorithms) and databases. These managed objects include those of SDPS and CSMS.

The Fault Management Application Service comprises the following functional sub-services:

- Fault Definition and Setup
- Fault Detection and Notification
- Fault Diagnosis, Isolation and Identification
- Fault Recovery
- Reporting

A context diagram for Fault Management Application Service is provide in Figure 5.2-2.

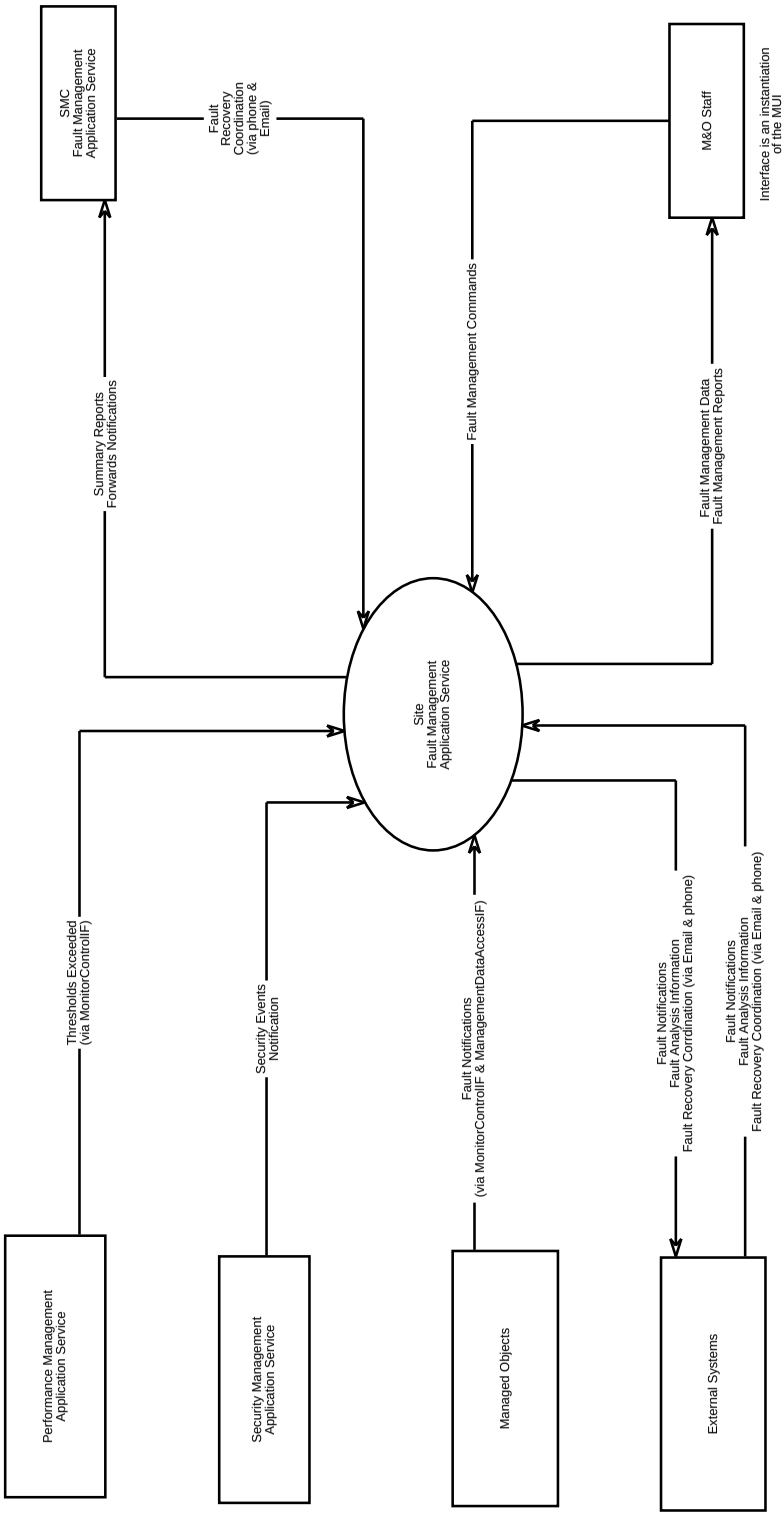

Figure 5.2-2. Fault Management Context Diagram

5.2.2.1 Fault Definition and Setup

5.2.2.1.1 Overview Fault Definition and Setup

In order to facilitate the detection of faults, certain preliminary tasks need to be performed. Events that constitute faults (device malfunctions, process failures, and conditions of degraded performance) need to be defined. The Fault Management Application Service provides the mechanisms that allow the definition of the events that need to be detected. These events include fault, failure, or performance degradation conditions.

For each of the defined events, the Fault Management Application Service provides the capability to specify detection mechanisms (the polling of a managed object by an agent or the polling of an attribute by the Fault Management Application Service), notification mechanisms (SNMP traps), polling frequency (where applicable, both by the Fault Management Application and by the agent), and the designated recipients of the notifications of the detected fault conditions. It provides mechanisms to enable or disable notifications to a disk log file or a display. It further provides the mechanisms by which categories of faults may be created, and by which individual faults may be assigned to those categories. This provides a method by which the M&O Staff can specify how different categories of faults will be handled once detected (whether or not the fault is reported to the fault management application immediately; whether it is reported to the site fault management application, EMC fault management application, or both; and whether the fault notification is imported into the management database.

For easy visual detection of the occurrence of faults, it uses the CMS MUI to organize the network topology into a presentable graphical display representation. The MUI allows the graphical representation to be divided into a series of displays, and further provides the capability to organize these series of displays into a hierarchy.

5.2.2.1.2 Fault Definition and Setup Functional Requirements

The following requirements specify minimum fault definition and setup capabilities:

C-MSS-60010 The MSS Fault Management Application Service shall provide the capability to create and display graphical representations of a given network topology consisting of the following:

a. routers

b. communication lines

c. hosts

d. peripherals

e. applications

C-MSS-60020 The MSS Fault Management Application Service shall provide the capability to define categories of faults.

C-MSS-60030 The MSS Fault Management Application Service shall provide the capability to assign faults to categories.

C-MSS-60040 The MSS Fault Management Application Service shall provide the capability to assign severity levels to faults.

C-MSS-60050 The MSS Fault Management Application Service shall be capable of providing the management data access service with a configurable list of fault categories that specify whether to enable or disable the logging of fault notifications for that fault category.

C-MSS-60060 The MSS Fault Management Application Service shall provide the capability to enable or disable the display of fault notifications received from a specific managed object based on fault category assigned to that fault.

C-MSS-60070 The MSS Fault Management Application Service shall provide the capability to specify additional information to be added to a disk log file, based on the fault category, when the notification of a fault is received.

C-MSS-60080 The MSS Fault Management Application Service shall have the capability to establish, view, modify and delete thresholds on performance metrics it measures.

5.2.2.2 Fault Detection and Notification

5.2.2.2.1 Overview Fault Detection and Notification

The detection of a fault may be performed in one of two ways: either by polling an attribute of a managed object or by the receipt of a notification from another entity. Fault detection may be accomplished by the Fault Management Application itself for network devices, or by an agent for defined managed objects to include processes databases, peripheral devices, or by an application (error conditions internal to an application).

The Fault Management Application Service provides several mechanisms for the notification of a detected fault. These include visual indications/notifications of changing an icon color, displaying a message in a pop-up notification window, logging the notification to a disk log file (with optional operator-specified information), or generating audible alerts. All fault notifications need to be logged for the purposes of record keeping, report generation and post processing.

5.2.2.2.2 Fault Detection and Notification Functional Requirements

The following requirements specify minimum fault detection and notification capabilities:

C-MSS-60100 The MSS Fault Management Application Service shall have the capability to poll for the detection of fault/performance information.

C-MSS-60110 The MSS Fault Management Application Service shall be capable of receiving fault notifications.

C-MSS-60120 The MSS Fault Management Application Service shall have the capability to define the frequency with which polling is done for the detection of fault/performance information.

C-MSS-60130 The MSS Fault Management Application Service shall provide the capability to detect the following types of faults, errors and events:

a. communications software version mismatch errors

b. communication software configuration errors

c. the following errors in communication hardware:

1. host not reachable
2. router not reachable
3. errors and failures of communication links

d. Errors in the communications protocols supported

e. degradation of performance due to established thresholds being exceeded

f. Peripherals:

g. Databases:

h. Applications:

1. process missing (Application or COTS product)
2. process in a loop
3. process failed

C-MSS-60140 The MSS Site Fault Management Application Service shall have the capability to generate a fault notification when a predefined threshold on a performance metric is exceeded.

C-MSS-60150 The MSS Fault Management Application Service shall have the capability to receive fault notifications from the Management Agent Service.

C-MSS-60160 The MSS EMC fault management application service shall have the capability to receive notifications of detected faults and degradation of performance from :

a. Site fault management applications

b. other external systems as defined in Section 5.1

C-MSS-60170 The MSS EMC fault management application service shall be capable of requesting fault notification and performance degradation data from :

a. Site fault management applications

b. other external systems as defined in Section 5.1

C-MSS-60180 The MSS EMC fault management application service shall be capable of receiving summarized fault notification and performance degradation data from :

a. Site fault management applications

b. other external systems as defined in Section 5.1

C-MSS-60190 The MSS Fault Management Application Service shall use the Logging Services to record each detected fault.

C-MSS-60200 The MSS Fault Management Application Service shall have the capability to generate the following types of notifications for detected faults :

a. a change in the color of an icon on a display

b. a message in a pop-up notification window

c. logging the following fault information to a disk log file:

1. fault type
2. date and time of occurrence of the fault
3. identification of the source of the notification (e.g. IP address, process name etc.)
4. fault data received with the notification
5. operator-defined descriptive text

d. audible alert

C-MSS-60210 The MSS Fault Management Application Service shall maintain a list of external service providers, M&O operators, and applications to be notified in the event that a specified fault is detected.

C-MSS-60220 The MSS Fault Management Application Service shall have the capability to send the notification of a fault to registered recipients.

C-MSS-60230 The MSS Fault Management Application Service shall have the capability of generating a notification within a maximum of five minutes of fault detection.

5.2.2.3 Fault Diagnosis, Isolation and Identification

5.2.2.3.1 Overview Fault Diagnosis, Isolation and Identification

The notification mechanism by which a detected fault is reported and the disk log files normally contain some amount of diagnostic information to help focus analysis efforts. Increasingly focused tests help localize the fault. For host-based, or service-based faults, analysis of the disk log files, in most cases, helps direct further analysis (e.g., analysis of a COTS product's logs).

For hardware-related faults, the execution of diagnostics provided by a vendor help characterize the nature of a fault. In other cases, it may be necessary to coordinate subsystem-level, site-level or system-level tests in order to localize and firmly identify a fault.

In order to facilitate the diagnosis, isolation and identification of a fault, the Fault Management Application Service provides several mechanisms. These include diagnostic tests, vendor-provided diagnostics and the disk log files that contain diagnostic information.

5.2.2.3.2 Fault Diagnosis, Isolation and Identification Functional Requirements

The following requirements specify minimum fault detection and notification capabilities:

C-MSS-60300 The MSS Fault Management Application Service shall provide the capability to identify routes between selected pairs of hosts on the ESN.

C-MSS-60310 The MSS Fault Management Application Service shall provide utilities to perform diagnostics and testing of the following for the purpose of fault isolation:

a. connectivity between pairs of ECS hosts and ECS routers

b. ability to reach hosts and routers

c. availability of network services at hosts

C-MSS-60320 The MSS Fault Management Application Service shall provide, for selective use as a debugging aid, the capability to perform packet tracing of protocols used in ECS.

C-MSS-60330 The MSS Fault Management Application Service at each site shall have the capability to perform periodic testing of all ECS communication links at that site to verify that they are operational.

C-MSS-60340 The MSS Fault Management Application Service shall be capable of verifying the operational status of a host.

C-MSS-60350 The MSS Fault Management Application Service shall have the capability to periodically execute diagnostic tests in order to isolate, characterize and identify a fault.

C-MSS-60360 The MSS Fault Management Application Service shall provide the capability to execute vendor diagnostics in order to diagnose faults traced to hardware equipment.

Note: These diagnostics will be limited to those made available by vendors. The diagnostic capabilities of these tools will be limited to the functionality as provided in these tools by the vendors.

C-MSS-60370 The MSS Fault Management Application Service at the SMC shall be capable of sending gathered isolation, location, identification and characterization of reported faults data to the level of subsystem and equipment to the following:

a. the site Fault Management Applications

b. other external systems as defined in Section 5.1

C-MSS-60380 The MSS Fault Management Application Service at the sites shall isolate, locate, and identify faults, identify subsystem, equipment and software faults, and identify the nature of the faults detected within its site.

C-MSS-60390 The MSS Fault Management Application Service at the sites shall, for faults detected within its site, isolate, locate, and identify faults to the level of:

a. subsystem

b. equipment

c. software

C-MSS-60395 The MSS Fault Management Application Service shall be capable of retrieving records of detected fault.

5.2.2.4 Fault Policies and Procedures

5.2.2.4.1 Overview Fault Policies and Procedures

The EMC is expected to distribute overall policies and procedures for Fault Identification and the subsequent recovery or corrective actions employed to recover from them. These policies are expected to flow down from the EMC to the sites for implementation.

5.2.2.4.2 Fault Policies and Procedures Functional Requirements

The following requirements specify minimum policies and procedures capabilities:

C-MSS-60400 The MSS EMC Fault Management Application Service shall support, maintain, and update system fault management policies and procedures, to include:

a. Fault Identification

b. Fault priorities

c. Recovery or corrective actions

C-MSS-60410 The MSS Site Fault Management Application Service shall have the capability to receive fault management policies and procedures from the EMC.

C-MSS-60420 The MSS Fault Management Application Service shall interface with the MSS Configuration Management Application Service and schedule a change in the configuration of the site when such a change in the configuration of the site is deemed necessary to recover from a fault.

5.2.2.5 Fault Recovery

5.2.2.5.1 Overview Fault Recovery

Once the exact nature of the fault has been determined, recovery procedures need to be initiated in order to restore the system to an operational state. These recovery procedures may be simple (the resetting of file permissions and restarting an application that aborted due to an error accessing a file), or more involved (scheduling corrective maintenance of failed equipment). In the latter case, some coordination with the Configuration Management Application may be necessary. Once the fault condition has been cleared, the failed component may be restored to an operational state.

5.2.2.5.2 Fault Recovery Functional Requirements

The following requirements specify minimum fault recovery capabilities:

C-MSS-60500 The MSS EMC Fault Management Application Service shall coordinate the recovery from conditions of performance degradation and faults with the sites and external network service providers.

C-MSS-60510 The MSS EMC Fault Management Application Service at the SMC shall coordinate, as necessary via directives and instructions, the recovery from faults reported from a site.

C-MSS-60520 The MSS Fault Management Application Service shall provide the capability to allow the specification and execution of action routines in response to the notification of a fault.

C-MSS-60530 The MSS Fault Management Application Service shall provide the capability to pass parameters to action routines.

C-MSS-60540 The MSS Fault Management Application Service shall utilize office automation support tools for the generation of directives and instructions for recovery from faults within its site.

5.2.2.6 Fault Reporting

5.2.2.6.1 Overview Fault Reporting

The gathered fault data will be reported to M&O Staff and external service providers in graphical and tabular format via the MUI. The Fault Management Application Service will also provide the M&O Staff with the ability to select and generate fault statistics (real-time and historical) for operator-selectable managed objects. These statistics will be displayable in either a tabular or a graphical format.

5.2.2.6.2 Fault Reporting Functional Requirements

The following requirements specify minimum fault reporting capabilities:

C-MSS-60600 The MSS Fault Management Application Service shall have the capability to generate, on an interactive and on a scheduled basis, reports on performance/error data that it has been configured to collect.

C-MSS-60610 The MSS Fault Management Application Service shall have the capability to build histories for different types of errors and events detected, for the purpose of analysis.

C-MSS-60620 The MSS Fault Management Application Service shall have the capability to redirect reports to:

a. console

b. disk file

c. printer

5.2.3 Performance Management Application Service

The MSS performance management application service will provide performance data monitoring, trending, testing, and reporting. The performance management application service will reside at the SMC and at the sites. The EMC performance management application service will be responsible for managing the performance of network managed objects (links, routers, bridges, and gateways), while the site performance management application service will be responsible for managing the performance of site elements (hosts, peripherals, LANs, databases, applications, and science algorithms). In addition, the EMC performance management application service will also receive summarized performance data from all sites and will be capable of retrieving specific performance data from a selected managed object at any site, per site policy agreements.

The MSS EMC performance management application service will manage the performance of ESN routers, bridges, gateways, links, and enterprise wide performance monitoring for all of ECS. The MSS site performance management application service will manage the performance of system components, consisting of hosts, peripherals, LANs, databases, applications, and science algorithms, that are located at the site.

A context diagram for Performance Management Application Service is provide in Figure 5.2-3.

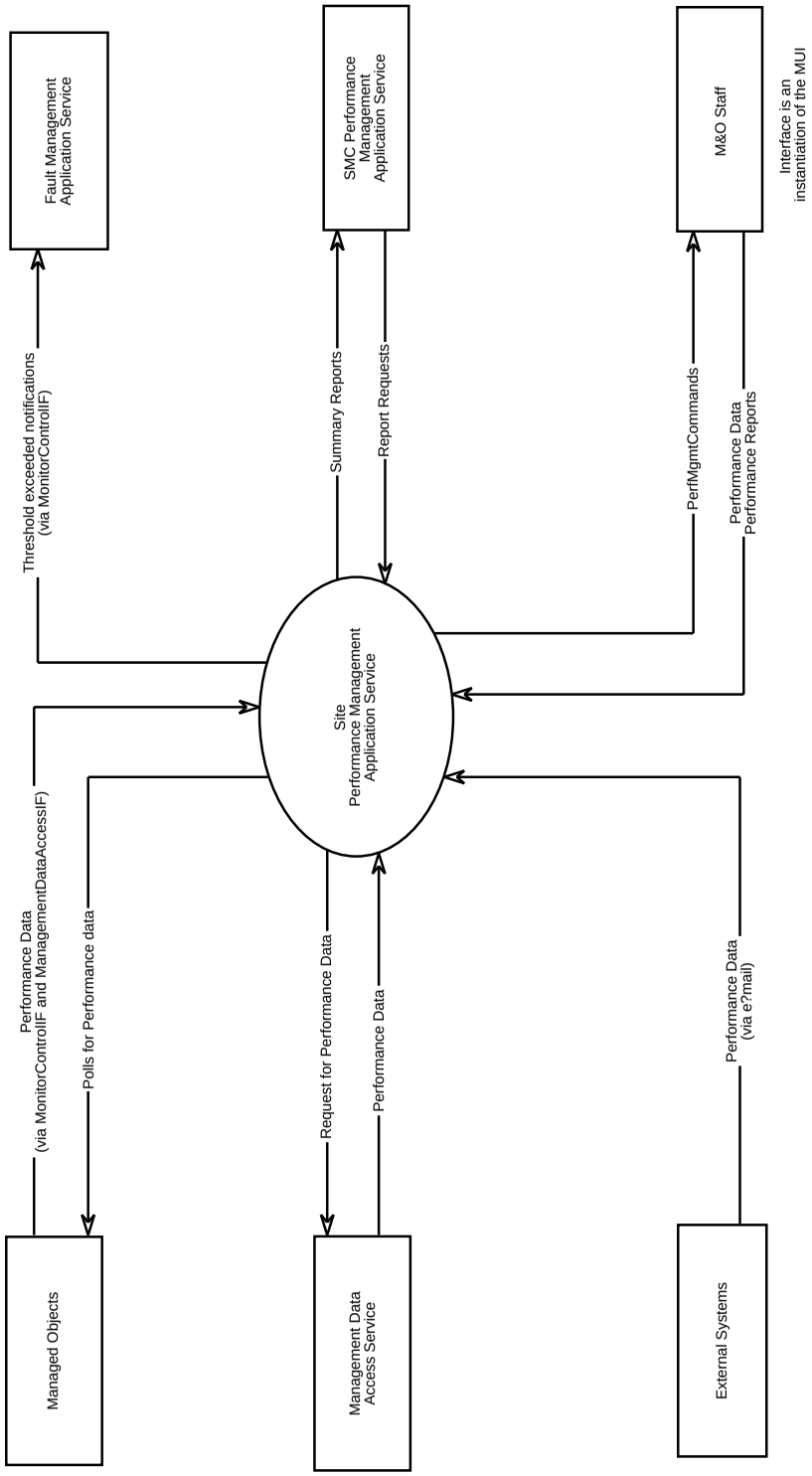

Figure 5.2-3. Performance Management Context Diagram

5.2.3.1 Performance Monitoring and Analysis

5.2.3.1.1 Overview Performance Monitoring and Analysis

Performance monitoring will involve the collection and analysis of performance data from managed objects throughout the ECS. Collection of performance data for all managed objects except science algorithms (for which the performance monitoring and analysis is discussed below) will be done through the monitoring service. For each managed object, a list of measurable performance parameters will be provided in the managed object definition. The actual performance parameters measured and the frequency of such measurements will be configurable by resource. The monitoring service will retrieve performance data from the managed objects, provide it to the performance management service for comparison against established thresholds, and store it in the History Log. The management data access service will transfer logged data into the Management Database so that it can be queried to generate operator-selected performance statistics. In addition, the performance data for a given site will be summarized and sent to the EMC on a periodic basis to provide the EMC with an overall view of system performance.

Performance monitoring of science algorithms will be handled differently. Algorithm performance data will be logged using APIs supplied by CSS in the SDP toolkit. The management data access service will transfer the logged data into the Management Database where the algorithm performance data can be browsed and analyzed and algorithm performance statistics can be generated at a later time.

5.2.3.1.2 Performance Monitoring and Analysis Functional Requirements

The following requirements specify minimum performance monitoring and analysis capabilities:

C-MSS-66000 The MSS Performance Management Application Service shall be capable of monitoring the performance of the following ECS components

a. network components
   1. routers
   2. links
   3. bridges
   4. gateways

b. hosts

c. operating systems

d. peripherals

e. databases

f. applications

C-MSS-66010 The MSS Performance Management Application Service shall be capable of monitoring ECS component protocol stack performance parameters defined in IETF RFC 1213.

C-MSS-66020 The MSS Performance Management Application Service shall be capable of monitoring ethernet-like device performance parameters as specified in IETF RFC 1623.

C-MSS-66030 The MSS Performance Management Application Service shall be capable of receiving managed object definitions for each managed object.

C-MSS-66040 The MSS Performance Management Application Service shall be capable of specifying which available performance metrics are to be gathered from each individual managed object.

C-MSS-66050 The MSS Performance Management Application Service shall be capable of requesting performance data from each individual managed object:

a. at configurable intervals

b. on demand.

C-MSS-66060 The MSS Performance Management Application Service shall be capable of receiving requested performance data from ECS components.

C-MSS-66070 The MSS Performance Management Application Service shall be capable of receiving unrequested performance data from ECS managed objects.

C-MSS-66080 The MSS Performance Management Application Service shall be capable of retrieving the following data for all network component interfaces:

a. operational status

b. type

c. speed

d. octets in/out

e. packets in/out

f. discards in/out

g. errors in/out

C-MSS-66090 The MSS Performance Management Application Service shall have the capability to collect the following performance information about communication protocol stacks on managed devices:

a. number of transport layer messages received with errors

b. number of transport layer messages requiring retransmission.

c. number of transport layer messages received that could not be delivered

d. number of network layer messages received with errors

e. number of network layer messages received that could not be delivered

f. number of network layer messages that were discarded

C-MSS-66100 The MSS Performance Management Application Service shall be capable of retrieving the following data for all hosts:

a. total CPU utilization

b. memory utilization

c. physical disk I/O's

d. disk storage size

e. disk storage used

f. number of active processes

g. length of run queue

h. network I/O's (packets)

i. network errors

C-MSS-66120 The MSS Performance Management Application Service shall be capable of determining the operational state of all network components, hosts, and peripherals to be:

a. on-line

b. off-line

c. in test mode

C-MSS-66130 The MSS Performance Management Application Service shall be capable of receiving operational state change notifications from network components, hosts, applications and peripherals.

C-MSS-66135 The MSS Performance Management Application Service shall have the capability to calculate the following statistics for the purpose of supporting RMA analysis for managed objects:

a. Mean Down Time (MDT)

b. Mean Time Between Maintenance (MTBM)

1. Mean Time Between Preventive Maintenance (MTBPM)

2. Mean Time Between Corrective Maintenance (MTBCM)

c. Mean Time To Repair (MTTR)

C-MSS-66137 The MSS Performance Management Application Service shall retain the calculated RMA statistics in a repository accessible for further analysis by the M&O Staff.

C-MSS-66140 The MSS EMC Performance Management Application Service shall have the capability to request performance data from :

a. Site Performance Management Applications

b. other external systems as defined in Section 5.1

C-MSS-66150 The MSS EMC Performance Management Application Service shall be capable of receiving performance data from :

a. Site Performance Management Applications

b. other external systems as defined in Section 5.1

C-MSS-66160 The MSS EMC Performance Management Application Service shall be capable of receiving summarized performance data from :

a. Site Performance Management Applications

b. other external systems as defined in Section 5.1

C-MSS-66170 The MSS Performance Management Application Service shall log ECS performance data pertaining to ECS network components and operating system resources.

C-MSS-66180 The MSS Performance Management Application Service shall have the capability to generate the following types of statistics for a configurable period of time for performance data stored in the Management Database:

a. average

b. median

c. maximum

d. minimum

e. ratios

f. rates

g. standard deviations.

C-MSS-66190 The MSS Performance Management Application Service shall provide a configurable number of thresholds for each performance metric.

C-MSS-66200 The MSS EMC Performance Management Application Service shall be capable of creating a list of suggested initial threshold values for each performance metric.

C-MSS-66210 The MSS EMC Performance Management Application Service shall be capable of sending a list of suggested initial thresholds for each performance metric to the MSS site Performance Management Application Service.

C-MSS-66220 The MSS site Performance Management Application Service shall be capable of receiving a list of suggested initial thresholds for each performance metric from the MSS EMC Performance Management Application Service.

C-MSS-66230 The MSS Performance Management Application Service shall allow each performance metric threshold to be configurable.

C-MSS-66240 The MSS Performance Management Application Service shall be capable of evaluating each performance metric against defined thresholds.

C-MSS-66250 The MSS Performance Management Application Service shall record an event in the local History Log whenever a threshold is crossed.

C-MSS-66260 The MSS Performance Management Application Service shall provide queries that generate performance statistics from performance data stored in the Management Database.

C-MSS-66270 The MSS Performance Management Application Service shall store generated performance statistics.

C-MSS-66280 The MSS site Performance Management Application Service shall be capable of extracting summarized site status information from logged performance data.

C-MSS-66290 The MSS site Performance Management Application Service shall be capable of sending summarized status information for that site to the MSS EMC Performance Management Application Service.

C-MSS-66300 The MSS EMC Performance Management Application Service shall log received summarized site status.

C-MSS-66310 The MSS Performance Management Application Service shall be capable of retrieving the following science algorithm performance data via the Management Data Access Service:

a. algorithm name

b. algorithm version

c. start time

d. stop time

e. CPU utilization

f. memory utilization

g. disk reads

h. disk writes

5.2.3.2 Performance Trending

5.2.3.2.1 Overview Performance Trending

In order to assist the M&O staff in spotting performance trends, the performance management application service will be capable of extracting from the History Log the measured values for any performance metrics gathered for specified managed objects over a specified period of time. The performance management application service will then allow the M&O Staff to browse through the performance metrics extracted, graphing the stored values against the time the values were obtained.

Note: Performance trending capabilities will be provided in Release A

5.2.3.2.2 Performance Trending Functional Requirements

The following requirements specify minimum performance trending capabilities:

C-MSS-67000 The MSS Performance Management Application Service shall be capable of extracting values of performance metrics gathered for a specified managed objects over a configurable period of time from the Management Database.

C-MSS-67010 The MSS Performance Management Application Service shall be capable of generating a graph of the extracted performance metric values.

5.2.3.3 Performance Reporting

5.2.3.3.1 Overview Performance Reporting

The gathered performance data and generated statistics will be reported to M&O staff and to SDPS subsystems (Ingest, Data Server, Client, and Data Processing). M&O staff will receive graphical displays of the currently reported state for each managed object. Each managed object will be represented by an icon whose color will denote the operational state of the object. The performance management application service will also provide the M&O staff with the ability to select and generate performance statistics for M&O Staff-selectable managed objects. These statistics will be displayable in either a tabular or a graphical format.

The performance management application service will also be capable of receiving and responding to requests from Ingest, Data Server, Client, and Data Processing subsystems for performance information associated with their objects.

Note: Performance reporting capabilities will be provided in Release A.

5.2.3.3.2 Performance Reporting Functional Requirements

The following requirements specify minimum performance reporting capabilities:

C-MSS-68000 The MSS Performance Management Application Service shall be capable of graphically displaying the operational state of managed objects through the MUI service.

C-MSS-68010 The MSS Performance Management Application Service shall be capable of displaying M&O Staff-selected performance statistics through the MUI in tabular and graphical formats.

C-MSS-68020 The MSS Performance Management Application Service shall be capable of printing M&O Staff-selected performance statistics.

C-MSS-68030 The MSS Performance Management Application Service shall be capable of receiving system resource utilization information requests from the SDPS Data Processing subsystem via the Management Agent Service.

C-MSS-68040 The MSS Performance Management Application Service shall be capable of providing the following current system resource utilization information to the SDPS Data Processing subsystem via Management Agent Service:

a. CPU utilization

b. memory utilization

c. disk I/Os (per second)

C-MSS-68050 The MSS Performance Management Application Service shall be capable of receiving resource utilization information requests from the SDPS Data Server subsystems via Management Agent Service.

C-MSS-68060 The MSS Performance Management Application Service shall be capable of providing the following current resource utilization information to the SDPS Data Server subsystem via the Management Agent Service:

a. CPU utilization

b. memory utilization

c. disk I/Os (per second)

C-MSS-68070 The MSS Performance Management Application Service shall be capable of receiving resource utilization information requests from the SDPS Client subsystem via the Management Agent Service.

C-MSS-68080 The MSS Performance Management Application Service shall be capable of providing the following current resource utilization information to the SDPS Client subsystem via the Management Agent Service.

a. CPU utilization

b. memory utilization

c. disk I/Os (per second)

C-MSS-68090 The MSS Performance Management Application Service shall have the capability to generate reports from collected management data.

C-MSS-68100 The MSS Performance Management Application Service shall have the capability to redirect reports to:

a. console

b. disk file

c. printer

5.2.3.4 Performance Testing

5.2.3.4.1 Overview Performance Testing

Network performance testing is required to ensure that networks are performing adequately and to predict the need for additional network capacity. Operational benchmark tests and benchmarks will be established by the policies and procedures management service.

Note: Performance testing capabilities will be provided in Release A.

5.2.3.4.2 Performance Testing Functional Requirements

The following requirements specify minimum performance testing capabilities:

C-MSS-69000 The MSS Performance Management Application Service shall maintain operational benchmark test procedures.

C-MSS-69010 The MSS Performance Management Application Service shall receive and maintain operational benchmark test results .

C-MSS-69020 The MSS Performance Management Application Service shall be capable of performing operational benchmark tests.

C-MSS-69030 The MSS Performance Management Application Service shall be capable of providing results of benchmark tests and results of predefined tests to the M&O staff for validation.

5.2.4 Security Management Application Service

The Security Management Application Service provides the mechanisms for the of audit information (partially addressed by the Accounting & Accountability Management Service), the detection of security events, the management of the security databases within ECS, and the

protection of ECS resources and user information. The major functions of the MSS Security Management Application Service are as follows:

User Registration (In IR-1 only)

Security Database Management

Audit Information Collection

Compliance Management

Intrusion Detection

Recovery

Reporting

A context diagram for Security Management Application Service is provide in Figure 5.2-4.

5.2.4.1 User Registration

5.2.4.1.1 Overview User Registration

The Security Administrator at each DAAC is responsible for establishing, managing and maintaining authorized user accounts, and for organizing user accounts into groups, based on affiliation to an organization or a project. User Registration is included in the Security Management Application Service only for IR-1. In Release A, User Registration is included in the Accounting & Accountability Application Service. The Security Management Application Service provides the capability for the management of user accounts.

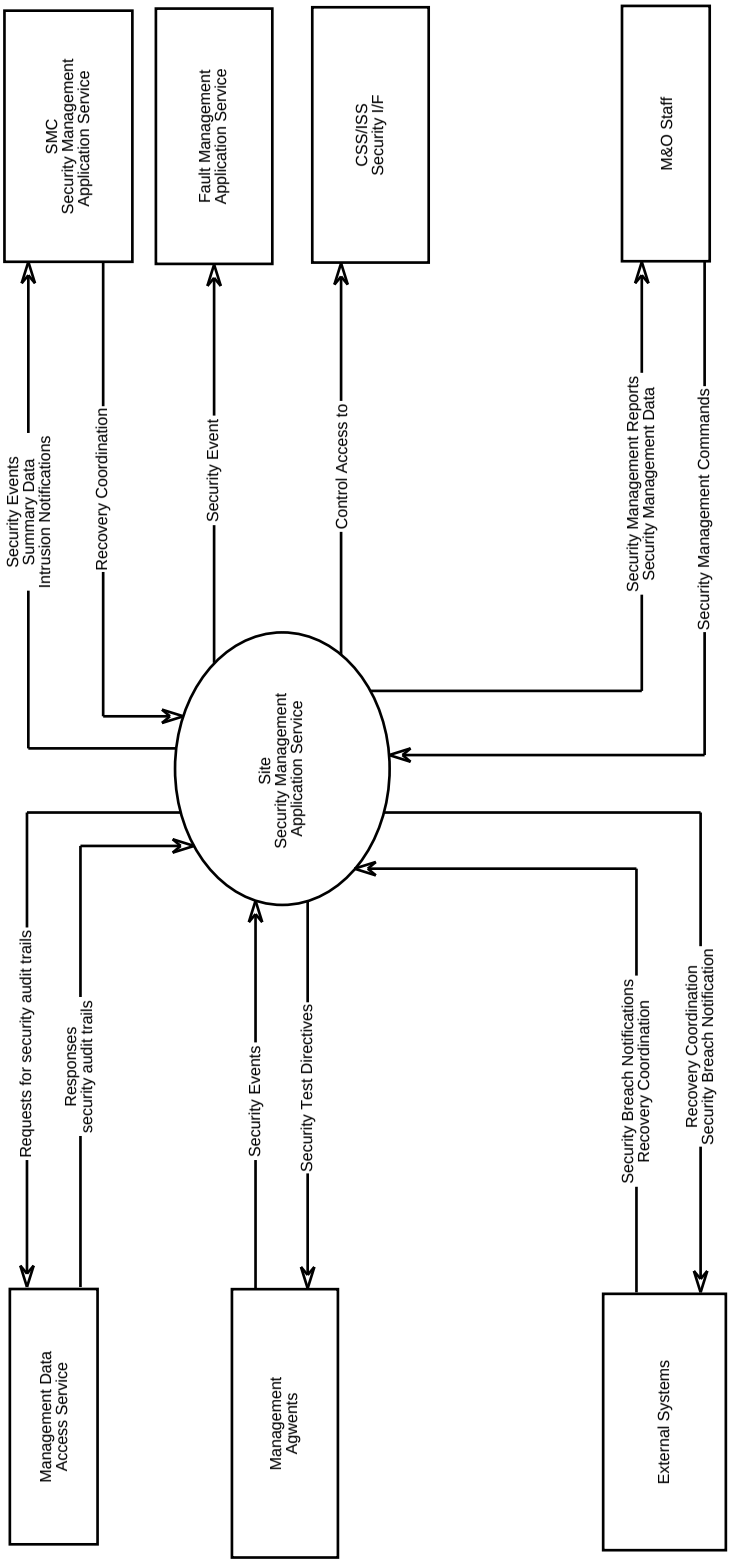

Figure 5.2-4. Security Management Context Diagram

5.2.4.1.2 User Registration Functional Requirements

The following requirements specify minimum user registration capabilities:

C-MSS-70010 The MSS Security Management Application Service shall provide the capability to create, modify and delete user accounts with the following attributes (IR-1 only)

a. username

b. password

c. group identification code

d. user identification code

e. login directory

f. command line interpreter

C-MSS-70020 The MSS Security Management Application Service shall enable the assignment of user accounts to groups based on the group identification code (IR-1 only).

5.2.4.2 Security Database Management

5.2.4.2.1 Overview Security Database Management

The MSS Security Management Application Service provides a command line interface and a graphical user interface, where possible, as the mechanisms for the management of the authentication and authorization databases. It also provides the mechanisms to establish, manage and maintain access controls on ECS resources based on group and user identification codes. This establishes the means by which access to ECS resources may be controlled.

NOTE: The security databases, the security audit trail, the accountability user and data audit trails, and configuration management data are special cases of ECS resources. As with all other ECS resources, the access to these resources needs to be restricted to authorized users. The Security Database Management function of the Security Management Application Service provide a uniform mechanism for the establishment, maintenance and management of the access control for all ECS resources.

5.2.4.2.2 Security Database Management Functional Requirements

The following requirements specify minimum security database management capabilities:

C-MSS-70100 The MSS site Security Management Application Service shall provide the capability to set, maintain, and update access control information for ECS resources.

C-MSS-70110 The MSS site Security Management Application Service shall provide the capability to specify privileges for authorized users and user groups for access to ECS resources.

C-MSS-70120 The MSS site Security Management Application service shall provide the mechanism, for each ECS host, to allow or deny incoming requests from specific hosts to services .

C-MSS-70130 The MSS site Security Management Application Service shall provide a command line interface and a GUI for the management of the following security databases:

a. Authentication Database

b. Authorization Database

c. Network Database

Note: A GUI for the network database will be provided as available in COTS.

5.2.4.3 Audit Information Collection

5.2.4.3.1 Overview Audit Information Collection

The Audit Information Collection for the Security Management Application Service is implemented within the Accounting & Accountability Application Service, but is briefly described here. The security audit trail generation mechanism is provided in order to collect and maintain security audit information for the purpose of analysis at each site. The security events that are recorded in this audit trail comprise authentication records, authorization records, and records pertaining to Compliance Management, and Intrusion Detection. Authorization records include those for a user requesting access to ECS services. Further, all incoming access to network services such as finger, telnet, FTP and rlogin on each ECS host need to be monitored and controlled based on the source of the access request. The security audit information collection mechanism facilitates the logging of all attempted accesses to network services such as finger, telnet, FTP and rlogin on each ECS host.

5.2.4.4 Compliance Management

5.2.4.4.1 Overview Compliance Management

The security policies implemented at each site need to be tested periodically in order to determine compliance to established policy. The Security Management Application Service provides the mechanism to determine this compliance to established policy. These mechanisms provide the capabilities to audit passwords, user privileges, access control information on ECS resources, and the integrity of file systems.

These mechanisms support Intrusion Detection.

5.2.4.4.2 Compliance Management Functional Requirements

The following requirements specify minimum compliance management capabilities:

C-MSS-70300 The MSS site Security Management Application Service shall have the capability to perform the following types of security tests:

a. password auditing

b. file system integrity checking

c. auditing of user privileges

d. auditing of resource access control information

C-MSS-70310 The MSS site Security Management Application Service shall have the capability to perform security testing on a periodic and on an interactive basis.

C-MSS-70320 The MSS site Security Management Application Service shall have the capability to send the results of the tests to the EMC Security Management Application Service.

C-MSS-70330 The MSS EMC Security Management Application Service shall have the capability to request, support, coordinate and maintain security testing for sites.

C-MSS-70340 The MSS EMC Security Management Application Service shall have the capability to request security testing of the sites on a scheduled and an interactive basis

C-MSS-70350 The MSS EMC Security Management Application Service shall have the capability to receive the results of security tests performed at the sites.

5.2.4.5 Intrusion Detection

5.2.4.5.1 Overview Intrusion Detection

The security audit trails at each site need to be audited periodically in order to detect intrusions into the system. Intrusions comprise files found to be modified at unauthorized times, excessive login failures, excessive authorization failures while attempting to access ECS resources, particularly security controlled resources such as the authentication and authorization databases. The Security Management Application Service will provide the mechanisms to analyze security audit trails in order to detect intrusions. It provides the mechanism to designate one or more users as recipients of a notification of the occurrence of such events, and the mechanism to provide the actual notification of the detection of these events to the designated recipients.

5.2.4.5.2 Intrusion Detection Functional Requirements

The following requirements specify minimum intrusion detection capabilities:

C-MSS-70400 The MSS EMC Security Management Application Service shall have the capability to receive notifications of security events from the site Security Management Application Services.

C-MSS-70410 The MSS EMC Security Management Application Service shall have the capability to receive security audit trails from the site Security Management Application Services.

C-MSS-70420 The MSS EMC Security Management Application Service shall have the capability to analyze security audit trails for the purpose of detecting intrusions.

C-MSS-70430 The MSS site Security Management Application Service shall provide the capability to designate a user or a group of users to receive a notification upon the detection of an intrusion, virus or worm..

C-MSS-70440 The MSS site Security Management Application Service shall provide the capability to notify designated M&O Staff(s) upon the detection of an intrusion, virus or worm.

C-MSS-70450 The MSS site Security Management Application Service shall have the capability to detect the following types of intrusions:

a. Login failures

b. Unauthorized access to ECS resources

c. Break-ins

d. Viruses and worms.

C-MSS-70460 The MSS site Security Management Application Service shall have the capability of generating a notification within a maximum of five minutes of the detection of an intrusion.

5.2.4.6 Security Recovery

5.2.4.6.1 Overview Security Recovery

Upon the detection and notification of a security event, recovery procedures need to be initiated in order to restore the system to an operational state. Security events may be local to a site, or they may affect more than one site. The Security Management Application Service provides the mechanisms to coordinate, via directives and instructions, the recovery from security events, and the restoration to a consistent state.

5.2.4.6.2 Security Recovery Functional Requirements

The following requirements specify minimum recovery capabilities:

C-MSS-70500 The MSS EMC Security Management Application Service shall have the capability to coordinate with the site Security Management Application Services, via directives and instructions, the recovery from security compromises.

C-MSS-70510 The MSS site Security Management Application Service shall, upon the detection of a compromise, isolate the compromised input I/O, and the compromised area's output I/O until the compromise has been eliminated.

C-MSS-70520 The MSS EMC Security Management Application Service shall provide office automation support tools to enable the generation of directives and instructions for recovery from detected security events.

C-MSS-70530 The MSS EMC Security Management Application Service shall coordinate, as necessary via directives and instructions, the recovery from security events reported from a site.

5.2.4.7 Security Policies & Procedures

The EMC is expected to establish overall policies and procedures for security management. These policies are expected to flow down from the EMC to the sites for implementation. The flow down of policy and procedures, in the IR-1 and Release A timeframe, will be performed by the M&O Staff using E-mail and Bulletin Board services.

5.2.4.8 Security Reporting

5.2.4.8.1 Overview Security Reporting

The capability to generate reports from the security audit trails will be provided by the SQL query and ad hoc report capabilities of a COTS DBMS that is specified in Section 5.2.1.6.

5.2.4.8.2 Security Reporting Functional Requirements

The following requirement specifies minimum reporting capabilities:

C-MSS-70700 The MSS Security Management Application Service shall have the capability to generate intrusion reports on the following:

a. Login failures

b. Unauthorized access to ECS resources

c. Break-ins

d. Viruses and worms

C-MSS-70710 The MSS Security Management Application Service shall have the capability to generate reports from collected management data.

C-MSS-70720 The MSS Security Management Application Service shall have the capability to redirect reports to:

a. console

b. disk file

c. printer.

5.2.5 Accountability Management Service

The accountability management service provides two basic functions: user registration and audit trails. The user registration will allow new users to be assigned privileges not provided to guest users while the audit trails (user, data, and security) will provide a record of events that have occurred within the system so that past activities can be reconstructed. A context diagram for Accounting Management Application Service is provide in Figure 5.2-5.

5.2.5.1 User Registration

5.2.5.1.1 Overview User Registration

The user registration function will allow a person to self-register in one of three ways: applying electronically by accessing the on-line user registration form available via the bulletin board service, completing it, and submitting it through e-mail; applying electronically by activating the "Register" function within the ECS Client Toolkit available on the bulletin board service; or by completing and submitting a 'New User Registration' package available at the site. Self-registration automates the collection of user information; it does not open an account. ECS operations staff must evaluate this information with respect to criteria prescribed in ECS policies before activating the new account and issuing a password. Approval to become a registered user is a manual process and will be performed at each site

Upon approval, the user's initial profile information will be entered into the system by the site's User Services Operator. The MSS User Registration capabilities will provide the interface for managing the registration process by the site's User Services Operator. The user registration interface will allow the entry of the user data into a database, assign a user class, and determine privileges. A user account will be created with an initial password.

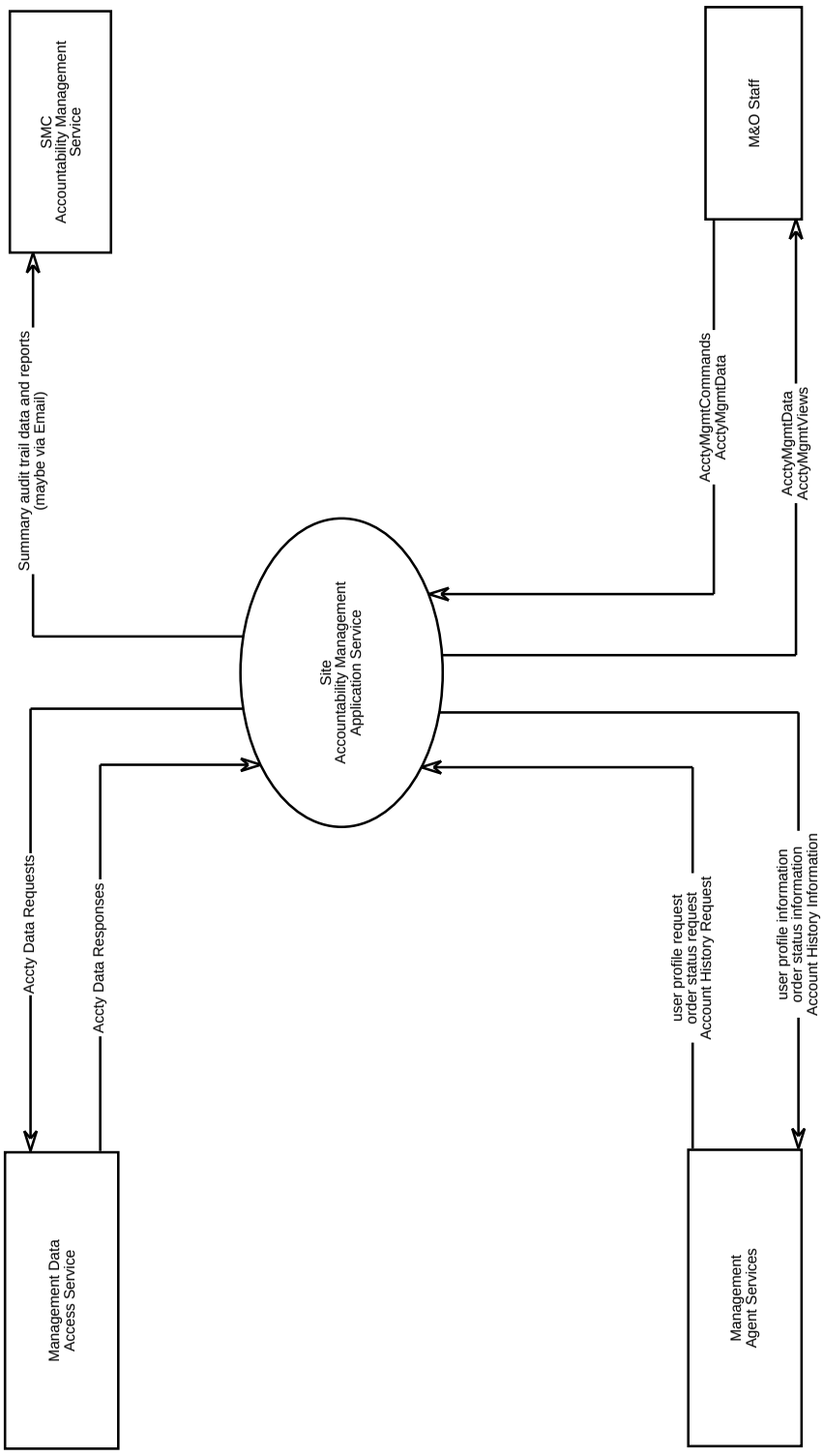

Figure 5.2-5. Accountability Management Context Diagram

The applicant for the new account will be notified by mail. The notification will include information regarding the initial system access procedures (including initial password), priority information, and authorized services will be provided. The user profile, created based on information provided by the user, will include:

- If applicable, name of the project for which the account is required, including the objective, duration, data requirements, and information to be derived.
- Name of the principal investigator including affiliation, full mailing address, telephone, and e-mail address.
- Names and addresses of co-investigators if separate user logon accounts are required. Product shipping address.

Note: Accountability management will be provided in Release A.

5.2.5.1.2 User Registration Functional Requirements

The following requirements specify minimum user registration capabilities:

C-MSS-75000 The MSS Accountability Management Service shall provide the capability to maintain a user profile database that stores the following information for each registered user:

a. Name

b. User ID

c. Password information
   1. password
   2. password expiration date

d. Assigned privileges

e. Mailing address

f. Telephone number

g. Product shipping address

h. E-mail address

i. Organization (optional)

j. Project affiliation(s) (optional)
   1. project name
   2. project principal investigator

k. User Group

l. Account information

1. creation date
2. expiration date

m. restrictions
   1. time of day
   2. location
   3. type of service

C-MSS-75010 The MSS Accountability Management Service shall be capable of receiving user profile records entered by M&O personnel.

C-MSS-75020 The MSS Accountability Management Service shall create a new user account whenever a new record is added to the user profile database.

5.2.5.2 User Audit Trail

5.2.5.2.1 Overview User Audit Trail

The user audit trail will track user access data including user id, class of user, time of each access or attempt to access ECS, duration of each session, and type of files accessed. The information will be logged by the SDPS subsystems each time a user attempts to logon or browse, search, or order data. The audit trail sub-service will coordinate with security services for security violations and for managing users account audits.

5.2.5.2.2 User Audit Trail Functional Requirements

The following requirements specify minimum user audit trail capabilities:

C-MSS-76000 The MSS Accountability Management Service shall be capable of retrieving user activity data (user id, type of user activity, data items used (browsed, searched, or ordered), and date/time of activity) from records generated by the SDPS Data Server, Data Processing, and Client subsystems.

C-MSS-76010 The MSS Accountability Management Service shall be capable of querying via the management data access service user activity data stored in the management database.

C-MSS-76020 The MSS Accountability Management Service shall be capable of retrieving all activities associated with a particular user or data item via the management data access service.

C-MSS-76030 The MSS Accountability Management Service shall log, for each ECS Host, incoming access attempts via:

a. telnet

b. FTP

c. rlogin

d. finger

C-MSS-76040 The MSS Accountability Management Service shall be capable of reporting audit information to M&O Staff via the MUI service.

5.2.5.3 Data Audit Trail

5.2.5.3.1 Overview Data Audit Trail

The data audits trail will record the progress of orders as they are processed through the system. As product generation activities are completed, a record of the completion will be entered in a history log. The user who ordered the product, the product ordered, the media type requested, the name of the completed activity, and the time required for the completed activity will be recorded.

5.2.5.3.2 Data Audit Trail Functional Requirements

The following requirements specify minimum data audit trail capabilities:

C-MSS-77000 The MSS Accountability Management Service shall be capable of retrieving data processing information (instrument used and date/time of ingest or algorithm used (name and version) and date/time or processing) from records generated by the SDPS Data Processing subsystem.

C-MSS-77010 The MSS Accountability Management Service shall be capable of querying via the management data access service all data processing information stored in the management database.

C-MSS-77030 The MSS Accountability Management Service shall be capable of retrieving all data processing information logged for a specified data item.

C-MSS-77040 The MSS Accountability Management Service shall be capable of accepting queries for the status of a particular ordered data item from the SDPS Client subsystem.

C-MSS-77050 The MSS Accountability Management Service shall be capable of interfacing with the SDPS subsystems to determine the status of an ordered data item to be:

a. Item in queue for processing

b. Item currently being processed

c. Item successfully processed

d. Error in processing

e. Error in request

C-MSS-77060 The MSS Accountability Management Service shall be capable of reporting the requested status of an ordered data item to the SDPS Client subsystem.

C-MSS-77070 The MSS Accountability Management Service shall be capable of searching local history logs to find processing data for an ordered data item.

C-MSS-77080 The MSS Accountability Management Service shall have the capability to generate reports from collected management data.

C-MSS-77090 The MSS Accountability Management Service shall have the capability to redirect reports to:

a. console

b. disk file

c. printer

5.3 Management Logistic Configuration Item (MLCI)

5.3.1 Configuration Management Application Service

5.3.1.1 Overview Configuration Management Application Service

ECS will employ a configuration management process to maintain the system's functional integrity throughout its lifecycle. The process entails knowing the parts of the system (including the characteristics of individual components and how components are collectively related) and systematically controlling their change. Resources that will be configuration managed include project deliverables such as custom software and COTS hardware and software, as well as non-ECS developed resources such as product generation algorithms. Site and SMC maintenance and operations staffs will rely on the Configuration Management Application Service (CMAS) to:

1. track what constitutes ECS deployed baselines
2. make descriptions of resource versions and status readily available
3. aid in managing system changes
4. store ECS source code, binaries, documentation, and other types of files in software libraries.

CMAS facilities will be distributed among the SMC and sites in support of both system-wide coordination and local system management respectively. Its control of software versions and its records of ECS configurations and change histories will facilitate the test, installation, trouble-shooting, maintenance, and operation of deployed resources and the migration of enhancements into the operational system.

CMAS is composed of several sub-services: baseline manager, software change manager, and change request manager. Functions of and requirements to be satisfied by these sub-services are presented below.

A context diagram for the Configuration Management Application Service is provided in Figure 5.3-1.

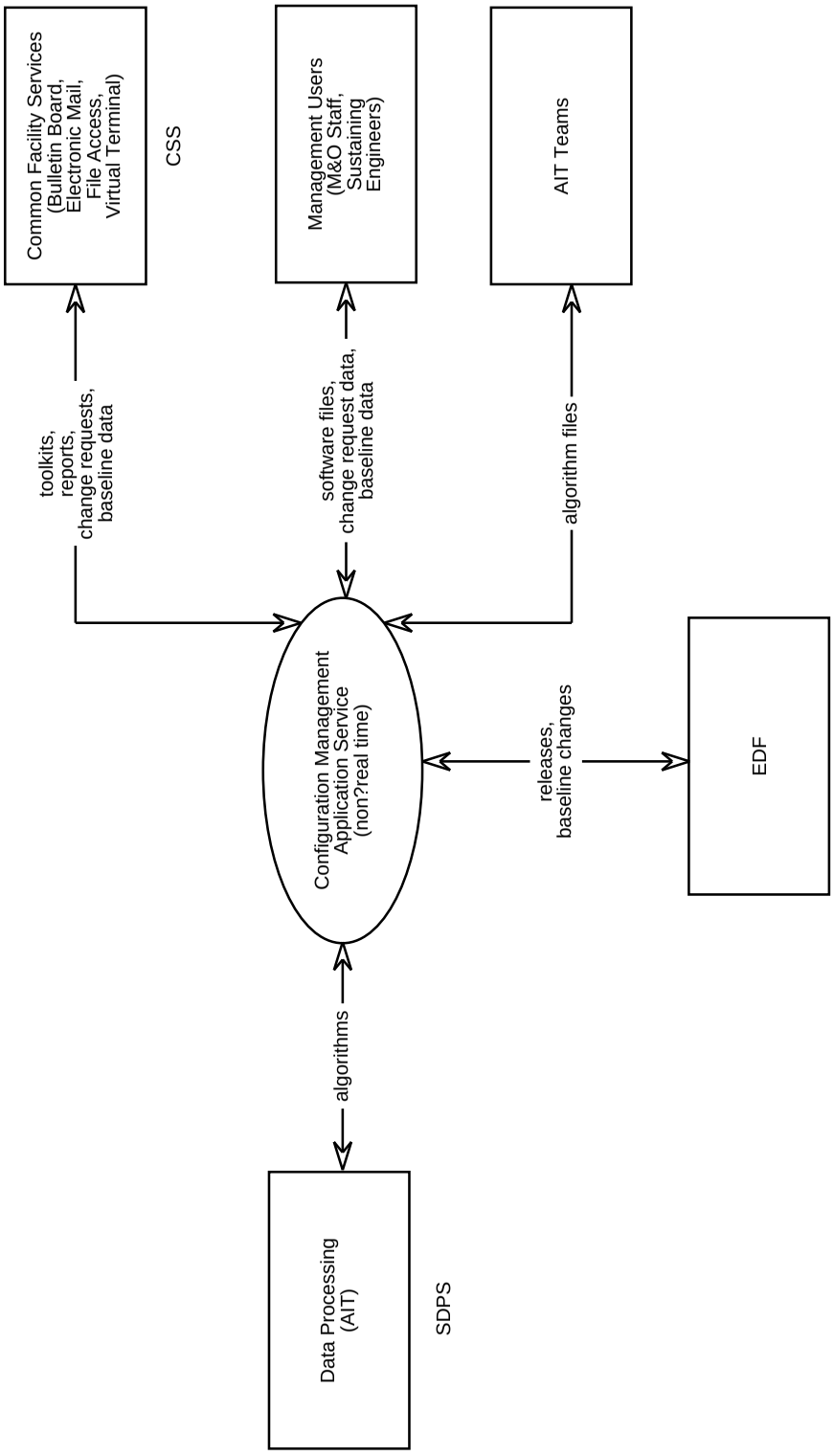

Figure 5.3-1. Configuration Management Context Diagram

5.3.1.2 Configuration Management Functional Requirements

5.3.1.2.1 Baseline Manager

The Baseline Manager tracks ECS baselines. It identifies what each released baseline contains, updates the status of its components, and establishes traceability between the baseline and the requirements and specifications its components are intended to meet. The Baseline Manager records all new baselines, traces them back to release baselines, and updates the status of their constituent resources. It catalogs configuration items and component parts of system devices, identifies relevant documentation for each system component, and maintains histories of changes to individual resources and to system and site configurations. Baseline Manager requirements are as follows:

C-MSS-40000 The MSS configuration management application service at each site shall track the following items at the site by name and identifier:

a. ECS subsystems, networks, and configured system and network devices such as workstations, servers, and routers;

b. ECS releases and site baselines;

c. ECS hardware and software resources designated as configuration items;

d. specifications associated with configuration items;

e. technical documentation and test materials

f. scientific algorithms, including software, data and test materials (DAACs only);

C-MSS-40010 The MSS configuration management application service at each site shall identify versions and variants of configuration controlled resources that comprise the site's operational baseline.

C-MSS-40030 The MSS configuration management application service at each site shall make available to the SMC records that identify the site's operational baseline and the versions and implementation status of configuration controlled resources that comprise it.

C-MSS-40040 The MSS configuration management application service at each site shall make available to the SMC "level of assembly" records that describe the composition of configuration items at the site.

C-MSS-40060 The MSS configuration management application service at each site shall maintain historical status records about ECS configuration items at the site, identifying each item's:

a. current version;

b. current version's specifications and technical, operations, and maintenance documentation;

c. specification and technical documentation history;

d. "level of assembly" representation of the components comprising the item's current and release configurations

e. version history.

C-MSS-40070 The MSS configuration management application service at the SMC and the sites shall maintain records that establish traceability among operational baselines and releases.

C-MSS-40080 The MSS configuration management application service at the SMC and the sites shall maintain records describing dependencies among baseline objects.

C-MSS-40100 The MSS configuration management application service at the SMC and the DAACs shall maintain SCF-provided configuration data for individual algorithms, including:

a. algorithm development version numbers, identification codes, and reference numbers;

b. SCF point of contact's name and organization;

c. associated files' names, formats, sizes, and descriptions;

d. number of files by category and type.

C-MSS-40110 The MSS configuration management application service shall display and report indentured, "level of assembly" lists that describe the component structure of configuration items.

C-MSS-40120 The MSS configuration management application service at the SMC shall track the names and identifiers of the following items deployed at the sites:

a. ECS subsystems, networks, and configured system and network devices such as workstations, servers, and routers

b. ECS releases and baselines;

c. ECS hardware and software resources designated as configuration items

d. specifications associated with configuration items;

e. technical documentation and test materials;

f. scientific algorithms, including software, data and test materials (DAACs only).

C-MSS-40140 The MSS configuration management application service at the SMC shall maintain, and make available system-wide, information identifying the sites where individual versions of configuration items are located and the operational status of that version at the site.

C-MSS-40150 The MSS configuration management application service at the SMC shall maintain, and make available system-wide, records that identify the current and previous versions of ECS hardware and software resources deployed to the sites.

C-MSS-40160 The MSS configuration management application service at the SMC shall maintain records that identify the current and previous versions of ECS documents associated with deployed ECS resources.

C-MSS-40170 The MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that identify the baseline changes included in each release of ECS hardware and software deployed to the site.

C-MSS-40180 The MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that identify the specifications and technical, operations, and maintenance documents associated with versions of ECS hardware and software configuration items deployed to the site.

C-MSS-40190 MSS configuration management application service at the SMC shall maintain, and distribute to each site, records that describe the change requests (enhancements and corrections) satisfied by new versions of ECS hardware, software, and documentation deployed to the sites.

C-MSS-40200 The MSS configuration management application service at the SMC shall maintain historical status records about ECS configuration items system-wide, to include each item's:

a. current version;

b. current version of specifications and technical, operations, and maintenance documentation;

c. specifications and technical documentation history;

d. "level of assembly" representation of components comprising the item's current and release configurations;

e. version history.

C-MSS-40210 The MSS configuration management application service at the SMC shall maintain historical status records about ECS system releases, to include each release's:

a. latest baseline plus approved changes;

b. baseline history;

c. latest release documentation;

d. "level of assembly" representation of the subsystem and configuration item versions that comprise the release configuration;

e. history of changes, including changes to subordinate units/components;

f. effectivity and installation status at operational sites;

g. release configuration.

C-MSS-40220 The MSS configuration management application service at the SMC shall maintain historical status records about ECS baseline changes to include:

a. sites affected;

b. installation dates;

c. installation status.

C-MSS-40240 The MSS configuration management application service at the SMC shall maintain software-critical and security-sensitive items lists.

C-MSS-40250 The MSS configuration management application service at the SMC shall produce, and make available system-wide, reports containing the identity and change status of documents associated with deployed ECS resources.

C-MSS-40260 The MSS configuration management application service at the SMC shall produce, and make available system-wide, reports, containing the identity and change status of individual ECS resources deployed to the sites.

C-MSS-40270 The MSS configuration management application service at the SMC shall produce, and make available system-wide, reports containing the identity of resources comprising ECS baselines and releases.

C-MSS-40280 The MSS configuration management application service shall characterize ECS-controlled resources as system-wide or site-specific.

C-MSS-40290 The MSS configuration management application service shall accept and store baseline management data records provided via interactive user interface and formatted data files.

C-MSS-40300 The MSS configuration management application service shall produce formatted data files containing baseline management data records.

5.3.1.2.2 Software Change Manager

The Software Change Manager organizes and partitions software, controls software changes and versions, and assembles sets of software for assigned releases. This manager stores software and associated files in a software library and controls changes to them. The Software Change Manager regulates access to source code, binaries, documentation, and other related files; journals changes to these files; and maintains resource and version associations. The Software Change Manager at the SMC will control the master, controlled versions of software released to the sites and the instructions and files used to assemble software packages for distribution. The Software Change Manager at each site will control the versions of ECS and science software at that site. Requirements associated with the Software Change Manager are listed below:

C-MSS-40400 The MSS configuration management application service at the sites and the SMC shall maintain software libraries to store files containing versions and platform variants of :

a. source code;

b. binaries and executables;

c. patches;

d. calibration coefficients and control data

e. scripts;

f. designs and design specifications;

g. databases;

h. technical documentation (both text and graphics);

i. test data;

j. test reports;

k. interface specifications;

l. configuration data. (IR-1)

C-MSS-40410 The MSS configuration management application service at each DAAC shall maintain user-definable software configuration status information for each algorithm. (IR-1)

C-MSS-40420 The MSS configuration management application service at each site shall maintain M&O staff-definable software configuration status information for each version of every software library file. (IR-1)

C-MSS-40460 The MSS configuration management application service at the SMC shall assemble unlicensed toolkit software files for posting to the ECS bulletin board. Files consist of:

a. source code;

b. linkable object code for selected workstation configurations;

c. makefiles that automate installation;

d. installation instructions.

C-MSS-40470 The MSS configuration management application service shall regulate operations on software library files through use of individual and group permissions.

C-MSS-40480 The MSS configuration management application service shall use a checkout/edit/checkin paradigm to govern changing of software library files.

C-MSS-40490 The MSS configuration management application service shall track each software library file that has been changed as a new version of the original file.

C-MSS-40500 The MSS configuration management application service shall merge versions of software library files and identify version conflicts, if any.

C-MSS-40510 The MSS configuration management application service shall maintain records of actual changes made to ECS software library files in implementing system enhancement requests.

C-MSS-40520 The MSS configuration management application service shall verify that changes to software library files are supported by approved change requests.

C-MSS-40530 The MSS configuration management application service shall identify implementation status for each version of every software library file, reflecting the lifecycle stage to which it has been promoted.

C-MSS-40540 The MSS configuration management application service shall perform builds of baseline systems for ECS platforms and audit the builds such that they can be repeated.

C-MSS-40550 The MSS configuration management application service shall reconstruct previous versions of software library files.

C-MSS-40560 The MSS configuration management application service shall allow concurrent user access to software library files.

C-MSS-40570 The MSS configuration management application service shall maintain an audit trail of all changes made to software library files.

5.3.1.2.3 Change Request Manager

The Change Request Manager will enable the M&O staff at the sites and SMC to register non-conformance reports and configuration change requests electronically. It will prompt for relevant information, assign identifiers, and mail requests to appropriate authorities. As change proposals and non-conformance reports advance through approval and implementation processes, the Change Request Manager will maintain status, disposition/resolution, approval, and closure information on-line as well as provide links to any associated change assessments. It will post relevant data for system-wide viewing so that the M&O Staff can access current, consistent information about each proposal's progress. Requirements for the Change Request Manager are listed below:

C-MSS-40600 The MSS configuration management application service shall provide a capability with which to specify a need for ECS system changes, both for enhancing system capabilities and for correcting non-conformance with system requirements.

C-MSS-40610 The MSS configuration management application service shall store copies of non-conformance reports and requests to modify ECS components and configurations.

C-MSS-40620 The MSS configuration management application service at the sites shall provide a capability with which to forward non-conformance reports and requests for ECS configuration changes to the SMC.

C-MSS-40650 The MSS configuration management application service at the SMC shall receive configuration change requests and non-conformance reports in electronic form from the sites.

C-MSS-40660 The MSS configuration management application service at the SMC shall distribute change evaluation requests to designated organizations system-wide and record evaluation assignments and distribution status.

C-MSS-40670 The MSS configuration management application service at the SMC shall receive and store impact assessments in response to change evaluation requests.

C-MSS-40680 The MSS configuration management service at the SMC shall electronically link impact assessments to their associated change requests.

C-MSS-40690 The MSS configuration management application service at the SMC shall maintain the status of responses to change evaluation requests.

C-MSS-40700 The MSS configuration management application service at the SMC shall record summaries of impact assessments received.

C-MSS-40720 The MSS configuration management application service at the SMC shall make non-conformance reports, configuration change requests, assessments, and status available for system-wide viewing.

C-MSS-40730 The MSS configuration management application service at the SMC shall maintain historical records of ECS configuration change requests, non-conformance reports, and system impact assessments.

C-MSS-40750 The MSS configuration management application service at the SMC shall track approval and closure status of configuration change requests and non-conformance reports.

C-MSS-40760 The MSS configuration management application service at the SMC shall report, and make available system-wide lists of the identity and disposition of configuration change requests and non-conformance reports against ECS baselines.

C-MSS-40770 The MSS configuration management application service at the SMC shall collect, and make available system-wide, the allocations, schedules and status of tasks for implementing CCB-approved changes to ECS hardware and software and for correcting non-conformance with system requirements.

C-MSS-40990 The MSS configuration management application service shall log the following information for configuration management events:

a. operation type;

b. userid of initiator;

c. date-time stamp;

d. host name. (IR-1, at the sites only)

C-MSS-40995 The MSS configuration management application service shall generate chronological reports of logged CM events associated with M&O staff-selectable:

a. time frames;

b. operation types;

c. userids;

d. hosts. (IR-1, at the sites only)

5.4 Management Agent Configuration Item (MACI)

5.4.1 Management Agent Service

5.4.1.1 Overview Management Agent Service

The enterprise management system, based on the manager/agent model, consists of a manager, an agent and a managed object. The manager provides the interface between the human network manager and the objects being managed. The agents are processes used to monitor and/or control managed objects distributed across heterogeneous platforms. The managed objects are the physical devices, the system software and the applications.

Current COTS technology for network management uses network protocols such as SNMP to provide a way for the manager, the managed objects, and their agents to communicate. SNMP defines specific messages, referred to as commands, responses, and notifications. The SNMP standard as specified in RFC 1157 has been selected as the ECS management protocol.

A context diagram for the Management Agent Service is provide in Figure 5.4-1.

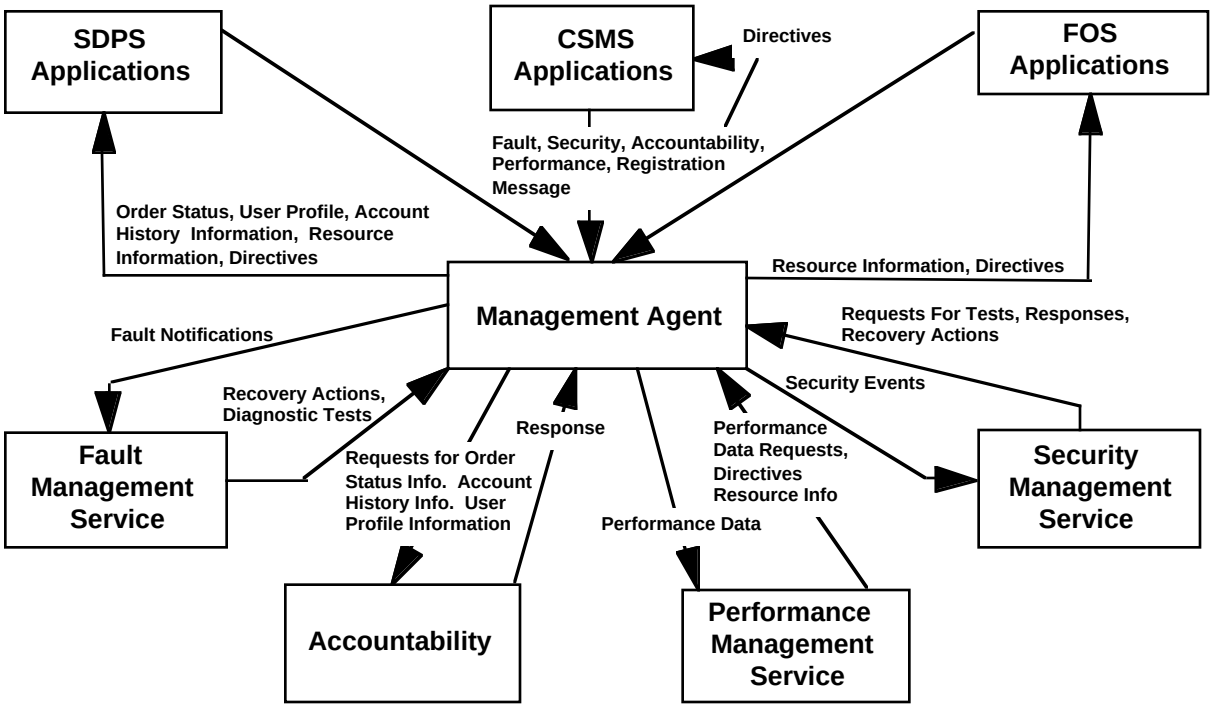

Figure 5.4-1. Management Agent Context Diagram

5.4.1.2 Management Agent Service Functional Requirements

C-MSS-36010 The MSS Management Agent Service shall retrieve data from ECS managed objects in test or operational mode.

C-MSS-36020 The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to respond to requests for managed object MIB attributes.

C-MSS-36040 The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to send ECS management traps/events to the Monitor/Control Service.

C-MSS-36050 The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to receive ECS management set message from the Monitor/Control Service.

C-MSS-36060 The MSS Management Agent Service shall provide an ECS management agent that is configurable to include:

a. Community to respond to and set attributes

b. Agent location & contact person

c. Traps to send

d. Events to log & log file name

C-MSS-36070 The MSS Management Agent Service shall provide an ECS management agent for network devices.

C-MSS-36080 The MSS Management Agent Service shall provide an extensible ECS management agent for ECS Host systems.

C-MSS-36090 The MSS Management Agent Service shall provide an extensible ECS management agent for ECS applications.

C-MSS-36100 The MSS Management Agent Service shall provide proxy agents for ECS network devices and applications that cannot be managed via SNMP.

C-MSS-36110 The MSS Management Agent Service shall provide an ECS domain manager agent to coordinate and communicate with multiple ECS management agents.

This page intentionally left blank.